iComplaints
PRIVACY IMPACT ASSESSMENT (PIA)

August 8, 2019

Office of Equal Employment Opportunity (OEEO)

Privacy Impact Assessment
iComplaints

Section 1: System Overview

1.1 Name of Project or System

iComplaints

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization) MicroPact, Inc.

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed: 1/10/2011

Last updated: 6/13/2017

Description of update: This PIA is being updated as part of continuous monitoring to ensure that current administrative and technical controls adequately protect the PII collected and that any new privacy risks are mitigated.

1.4 Does the system or program employ any of the following technologies?

☐ Enterprise Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☒ Cloud Computing Services

☐ www.sec.gov Web Portal

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

The Securities and Exchange Commission, Office of Equal Employment Opportunity (OEEO) provides a neutral and impartial forum for employees, former employees, and applicants for employment to file complaints of discrimination based on one or more of the protected equal employment opportunity (EEO) bases. To carry out its functions, OEEO uses the iComplaints system to track complaints and supporting documentation relating to employment discrimination, retaliation, and alternative dispute resolution matters. iComplaints permits OEEO staff to (1) maintain an electronic system of records for EEO complaints and related information, (2) ensure the accuracy, integrity, and security of personally identifiable information (PII) contained in the complaints, (3) assign and track complaints, (4) assist with timely complaint processing and notifications to complainants (i.e., track and monitor the location, status, and length of time elapsed at each stage of the complaint resolution process), (5) capture complaint processing costs and other data for trends analysis, (6) provide users remote access to complaints information in a secure environment, and (7) satisfy SEC continuity of operations plans. iComplaints is hosted by an off-site vendor, MicroPact Engineering, Inc.

OEEO has approved a limited number of staff as authorized users of the system. When a person wishes to enter the EEO process, an OEEO approved user will enter or upload information into iComplaints. The complainants do not have direct access to the system. The information contained in the system contains the PII of current and former employees, applicants who file complaints of discrimination or who are seeking resolution to

employment issues and related individuals. The information collected will vary based on the type of complaint or process undertaken. Administration of this system is crucial to the timely adjudication of the rights of all individuals involved in the complaint process.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Pursuant to 42 U.S.C. §§ 2000e-5(b), 42 U.S.C. §§ 2000e-16(a), (b) and (c) and 29 CFR 1614.102, this information is collected to create a factual record to adjudicate EEO complaints in a timely manner, order relief if appropriate and prepare reports mandated by the EEOC.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No
☐ Yes

If yes, provide the purpose of collection:
If yes, provide the legal authority:

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN

EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, 71 FR 24704 (April 26, 2006).

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No
☐ Yes

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The privacy risk associated with the purpose of the collection is that unauthorized users may view stored information or use the information for reasons not consistent with the original purpose. To mitigate this risk access is limited to those who need to know the information to perform job functions based upon pre-defined user roles and permissions. Account access privileges are based on the minimum access required to effectively perform the job functionality of the user. MicroPact's IT Operations team will monitor and review all accounts on quarterly basis and disable and /or revoke permissions for privileged accounts when no longer needed. The MicroPact IT Operations team is notified via an account request form and HR (email) when changes occur.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

The information contained in the system concerns current and former employees and applicants who file complaints of discrimination or who are seeking resolution to employment issues. The information collected varies based on the type of complaint or process undertaken. The most commonly found data elements have been identified below.

Identifying Numbers

☐ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☐ Financial Transactions
☐ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☒ File/Case ID	☐ Credit Card Number	☐ Employer ID
☒ Other:		

General Personal Data

☒ Name	☒ Date of Birth	☐ Marriage Records
☒ Maiden Name	☐ Place of Birth	☐ Financial Information
☒ Alias	☒ Home Address	☒ Medical Information
☒ Gender	☒ Telephone Number	☒ Military Service
☒ Age	☒ Email Address	☐ Mother's Maiden Name
☒ Race/Ethnicity	☒ Education Records	☒ Health Plan Numbers
☐ Civil or Criminal History	☒ Zip Code	
☒ Other: Religion and Pregnancy		

Work-Related Data

☒ Occupation	☒ Telephone Number	☒ Salary
☒ Job Title	☒ Email Address	☒ Work History
☒ Work Address	☒ Certificate/License Number	☒ Business Associates
☐ PIV Card Information	☒ Fax Number	
☒ Other: Division, Office		

Distinguishing Features/Biometrics

☐ Fingerprints	☒ Photographs	☒ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		

System Administration/Audit Data

☒ User ID	☒ Date/Time of Access	☒ ID Files Accessed
☒ IP Address	☒ Queries Ran	☒ Contents of Files
☐ Other:		

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

PII is collected to process and adjudicate EEO complaints, associate filers with their respective complaints, to avoid mishandling a complaint (i.e., an improper disclosure of complaint matters to the wrong complainant or mix-up of complaint matters), and to maintain current contact information for complainants, witnesses and representatives. Data is also being collected to process complaints in a timely manner, develop adequate factual records, issue decisions that are consistent with acceptable legal standards, explain the reasons for its decisions, and to give complainants adequate and timely notice of their rights. Data may also be used for reporting and statistical purposes. When used for statistical purposes, personal identifiers will be removed.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees

Purpose: PII may be collected or maintained on SEC employees to assist with processing and adjudicating EEO complaints.

☒ SEC Federal Contractors

Purpose: PII may be collected or maintained on SEC Federal Contractors to assist with processing and adjudicating EEO complaints.

☒ Interns

Purpose: PII may be collected or maintained on SEC Interns to assist with processing and adjudicating EEO complaints.

☐ Members of the Public

Purpose:

☒ Employee Family Members

Purpose: PII may be maintained on an employee's family members to assist with processing and adjudicating EEO complaints when a family member serves as representative for the filer or on behalf of a filer's estate.

☒ Former Employees

Purpose: PII may be collected or maintained on former employees to assist with processing EEO complaints filed by former employees.

☒ Job Applicants

Purpose: PII may be collected or maintained on job applicants to assist with processing EEO complaints filed by applicants for employment with the SEC.

☒ Vendors

Purpose: PII may be maintained on vendors that are used for counseling, mediation, investigations or final agency decisions stages of the EEO process.

☒ Other: Representatives

Purpose: PII may be maintained on agency representatives, attorneys and other individuals who represent a filer.

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

PII is limited to only the data necessary to process or adjudicate EEO complaints and investigations. Any PII collected will not be used for testing, training, and/or research efforts.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☐ No

☒ Yes

Records fall under the NARA General Records Schedule 1, Civilian Personnel Records, Item 25, Equal Employment Opportunity (EEO) Records, Sections a, b, c. Records must be retained for four years after the end of the year that the case closes and may be converted to statistical information and retained for an additional five years.

3.6 What are the procedures for identification and disposition at the end of the retention period?

The OEEO Records Liaison will coordinate with OEEO staff to develop and maintain a current inventory sheet of all EEO records. The OEEO Records Liaison will review the inventory sheet and coordinate the disposition of all EEO records with the OEEO Director, OEEO Compliance Lead, Office of the General Counsel, Office of FOIA Services and the Office of Records Management Services prior to the disposition of any record.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

. ☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

There is a risk that information not required to process or adjudicate an EEO complaint may be erroneously scanned or attached to a file in iComplaints. To mitigate this only certain OEEO employees have access to the iComplaints system based on predefined access roles. Those employees are thoroughly trained on the proper handling of EEO data.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☒ Privacy Act Statement
Individuals are provided notice on the formal EEO complaint form.

☒ System of Records Notice
EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeals Records.

☐ Privacy Impact Assessment
Date of Last Update: 11/19/2010

☐ Web Privacy Policy

☐ Other notice:

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

All SEC employees, former employees, applicants for employment, interns and contractors, who initiate the EEO process, receive notice that PII will be collected during the course of their EEO complaints and their information will be included in an agency system of records. They also receive notice that their PII will be safeguarded and treated as confidential information made available only to those with a need to know and in the course of official business. No risks regarding the adequacy of the Privacy Act notice were identified and the notice is being reviewed for enhancements. The risk of any departures from this process are mitigated by the annual mandatory privacy training that all OEEO staff take and the commitment by OEEO staff to adhere to the Privacy Act and internal procedures for processing EEO complaints. Further, OEEO is leveraging technology to enhance its delivery of privacy notices to individuals who enter the EEO complaints process, representatives and witnesses.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

iComplaints may aggregate data in order to generate ad hoc reports. When this happens, PII will be redacted from the report before the report is submitted to internal offices and external agencies.

5.2 Will internal organizations have access to the data?

☐ No
☒ Yes

Organizations: Internal organization such as OGC, OIG, OHR and the union may have a need to know information related to EEO complaints. Any information that is provided to these internal organizations is approved for release by the OEEO Director or designee. These organizations do not have permissions and roles to access iComplaints data directly and must request this data by e-mail, in-person or via telephone. OEEO determines the scope and release of such information.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

A privacy risk associated with internal sharing is that PII could be inadvertently disclosed to persons who have no need to know the information or who are not processing EEO complaints as part of their official duties. This privacy risk is mitigated as iComplaints is only accessible from within the SEC network and only available to OEEO staff that have permissions and roles to access the confidential and sensitive data. User permissions and roles are controlled by an OEEO Systems Administrator and a Micropact Systems Administrator, who can add users, change access levels and detect and remove unauthorized users.

5.4 Will external organizations have access to the data?

☒ No
☐ Yes

Organizations: Generally, external organizations such as Congress, GAO, DOJ, OPM and the EEOC do not have direct access to the data contained in iComplaints. These organizations receive and may request reports from OEEO that present the aggregate data in a narrative or statistical report.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

The external sharing of information brings about the risk of deliberate or accidental exposure of personal information. As mentioned above, external organizations do not have permissions to access iComplaints. Reports to external organizations that include data from iComplaints include the data in the aggregate in narrative or statistical reports and all PII is removed. Upon a request to OEEO, PII and routine information (i.e., case name, case number and status) can be shared with an external organization via letters, e-mails or telephone calls and the identity of the recipient or requestor must be known and verifiable.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☒ Other source(s): The filer's representative and witnesses to the complaint.

6.2 What methods will be used to collect the data?

Information pertaining to the claims and issues raised within the complaint is collected primarily from complainants, co-workers, supervisors, witnesses and legal representatives with knowledge of the allegations of discrimination. Information is acquired from individuals who initiate contact with OEEO and supply background information to support allegations of discrimination.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

The accuracy and completeness of the data collected from filers will be confirmed by OEEO staff, any affidavits that filers provide, information received from their representatives and information obtained from witnesses. Information collected directly from an individual is presumed to be accurate. When an individual completes the initial intake form for an EEO complaint, they are required to certify that the foregoing information is true and accurate to the best of their knowledge.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No
☐ Yes
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

Risks related to the method of collection and data quality and integrity are minimal. Information pertaining to the claims and issues raised within the complaint is collected primarily from complainants, co-workers, supervisors, witnesses and legal representatives with direct knowledge of the allegations of discrimination. Individuals who submit the information certify that the information is accurate to the best of their knowledge. Additionally, OEEO staff, who have permissions and roles to use iComplaints undergo training and have access to the iComplaints self-guided training to maintain the quality and integrity of data entries into iComplaints.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Individuals who contact OEEO may decline to provide requested information, but doing so may result in the dismissal of their allegation(s) because of failure to respond or proceed in a timely fashion. Individuals consent to the use of the information to the extent the information is used for EEO purposes.

7.2 What procedures are in place to allow individuals to access their information?

OEEO does not have procedures in place for individuals to access their data directly. However, upon request, OEEO can accept and make corrections to information and provide individual printouts of information from iComplaints. Persons wishing to obtain information on the procedures for gaining access to the contents of records may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

7.3 Can individuals amend information about themselves in the system? If so, how?

The SEC does not allow individuals access to their information stored in iComplaints through either the Internet or Intranet. Individuals seeking to amend the contents of records may contact the FOIA/Privacy Act Officer, Securities and Exchange Commission, 100 F Street, N.E., Washington, D.C. 20549-2736.

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

Individuals have the ability to ensure the accuracy of the information collected about them. Any risks that the individual will not be given the opportunity to correct their information is mitigated by allowing individuals who have privacy concerns to contact SEC FOIA/ Privacy Act Officer.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
SA&A Completion Date: 7/3/2019
Date of Authority to Operate (ATO) Expected or Granted: 7/3/2019
☐ No

8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

☒ Users
Roles: OEEO counselors, who conduct counseling sessions; OEEO ADR staff, who oversee mediations; OEEO attorneys, who manage/process EEO complaints; and OEEO staff, who otherwise assist with processing EEO complaints.

☒ Contractors
Roles: OEEO contractors who assist OEEO staff with processing EEO complaints; SEC/OIT contractors who access iComplaints data for development purposes.

☒ Managers
Roles: OEEO Director and OEEO Deputy Director, who access iComplaints data to manage, process review complaints and run reports.

☐ Program Staff
Roles:

☒ Developers
Roles: SEC/OIT employees who access iComplaints data for development purposes.

☒ System Administrators
Roles: OEEO Systems Administrator, who grants access to users; Micropact Systems Administrator, who grants access to users and provides higher level assistance such as system checks, data integrity and process improvement.

☐ Others:
Roles:

8.3 Can the system be accessed outside of a connected SEC network?

☒ No
☐ Yes

If yes, is secured authentication required?	☐	No	☐	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☐	Yes	☐	Not Applicable

8.4 How will the system be secured?

The MicroPact Physical Environment Security Policy ensures among other things that physical access to information systems, equipment and the operating environment is limited to authorized individuals and that information systems are protected from environmental hazards. The system uses a numeric field to identify unique individuals within the system. The system name for this field is the Unique ID (UID) field. The value in this field is a unique system-generated number that is not the same as, or based on any PII including any employment identification numbers or Social Security numbers. The system has other controls that mitigate privacy risks, which include:

- Users are assigned passwords, which expire after a set period. Minimum length of passwords is eight characters.
- Accounts are locked after a set period of inactivity.
- Accounts are locked after a set number of incorrect attempts.
- Security controls such as separation of duties, managing credentials and secure storage of backup media. The security controls protect the information while it is not being processed or transmitted.
- Database backups and all data transmissions are encrypted using UniTrends with FIPS 140-2 compliant encryption.
- Data transmitted over the internet is encrypted.
- The MicroPact Production Network utilizes a FIPS 140-2 compliant cryptography to authenticate users to the network via Active Directory.
- Authentication to the MicroPact Product Suite occurs through a FIPS 140-2 compliant Transport Layer Security (TLS)/Secure Socket Layer connection utilizing a 256-bit AES Encryption. Connection to the authentication mechanism occurs once the application server certificate is validated as being signed by a Trusted Third-Party Certificate Authority

MicroPact's production network has multiple tools in place for monitoring and intrusion detection. Firewalls monitor inbound and outbound communications for unusual or unauthorized activities or conditions in near real time. The Firewalls are configured to send out an automated alert if a configured alert condition is met. MicroPact utilizes Nessus Security Center's IDS functionality to detect, review, and respond to suspicious activities. Additionally, Solarwinds monitors servers' network health, web sites, and network devices and provides near real-time alerts when indications of compromise or potential compromise occurs.

MicroPact's IT Operations team also employs a wireless intrusion detection tool to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system (i.e., unauthorized changes to software and information, information tampering) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

8.5 Does the project or system involve an online collection of personal data?

☒ No
☐ Yes
Public
URL:

8.6 Does the site have a posted privacy notice?

☐ No
☐ Yes
☒ N/A

8.7 Does the project or system use web measurement and/or customization technologies?

☒ No
☐ Yes, but they do not collect PII

☐ Yes, and they collect PII

8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The privacy risk identified is inadvertent or unauthorized access/disclosure of nonpublic information. However, the risk is mitigated by (1) storing only necessary information in the system; (2) requiring each authorized user to log in with their own username and password via an SSL encrypted connection from browsers on their SEC computers over the Internet; (3) utilizing granular access controls (by group, user type, case type, and/or record type) to protect the data at all levels and (4) reviewing audit logs for unusual activity.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

SEC employees, interns and contractors with access to iComplaints must take annual mandatory privacy and security training. In addition, iComplaints self-guided training is available based on user roles, e.g., Case Processor, Case Manager, EEO Counselor, EEO Investigator, OGC Counsel, and Systems Administrator.

9.2 Does the system generate reports that contain information on individuals?

☐ No
☒ Yes

Ad-hoc reports may be generated for internal use. In this instance, information is in the aggregate, narrative or statistical format.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☒ Yes
☐ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

Based on current threat information and ongoing assessment of risk, the following events are to be audited within the iComplaints:

- Account logon events – Success and Failure
- Account management – Success and Failure
- Directory Service Access – Success and Failure
- Logon Events – Success and Failure
- Object Access – Success and Failure
- Policy Change – Success and Failure
- Privileged Use – Success and Failure
- Process Tracking – Success and Failure
- System Events – Success and Failure

These events are audited on a monthly basis or a frequency defined by Micropact. Audits are examined to determine if there have been any trends, anomalies or malicious/unlawful activity that needs to be communicated with the Systems Administrator or with the MicroPact Information Security Team. Authorized personnel can only access audit records. For the MicroPact Production Network, only the IT Operations Team and Database Administration Team have access to audit logs generated by the OS,

databases and network level activity. Original content of audit logs cannot be altered. The iComplaints Audit records are mirrored to the backup audit storage in near real-time capacity. MicroPact at this time keeps audit records in a period of perpetuity. Backups of audit records are also performed from virtual tapes to hard disk. The MicroPact team manages these backup files. Audit records are kept for ninety (90) days for the iComplaints application. Audit tools automatically alert the MicroPact IT Operations Team when the log storage reaches near capacity; the logs are then moved to physical media and stored in a secure location. These logs are easily accessible for review to provide support for after-the-fact investigations of security incidents and meet regulatory and client information retention requirements.

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

As previously mentioned, MicroPact's IT Operations team employs a wireless intrusion detection tool to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system (i.e., unauthorized changes to software and information, information tampering) and uses tools to automatically monitor the integrity of the information system and the applications it hosts. Further, all Micropact security reports will be labeled "For Official Use Only". MicroPact will notify the Contracting Officer's Technical Representative upon discovery of any inadvertent disclosures of information.

9.6 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Due to the sensitivity of EEO complaints, there is always a residual risk when any information is accessed or disclosed without authorization. Those risks include a challenge to the integrity of iComplaints, OEEO staff and OEEO. The established safeguards and manner of use described in this PIA are adequate to protect the sensitivity of PII stored in the system.