Privacy Impact Assessment (PIA)

for the

iComplaints

May 20, 2021

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Steven Jefferson
Contact Email: Steven.Jefferson@ed.gov

System Owner

Name/Title: Lee Flowe, Director Shared Services Systems Support Division
Principal Office: Office of Finance and Operations

Please submit completed Privacy Impact Assessments to the Privacy Office at
privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Electronic Case Management Platform (ECAMP) was developed to support the Office of Finance and Operations (OFO) strategy of streamlining information technology (IT) operations to better align with the U.S. Department of Education's (Department) goal of IT modernization, standardize the use of IT shared services, and reduce the overall cybersecurity footprint. The ECAMP will combine separate case management systems or modules, each with separate small contracts with Tyler Technologies, Inc. (formerly MicroPact), a cloud service provider (CSP).

iComplaints is a web-based application that is platform-independent of other user operating systems (i.e., iOS, Windows). iComplaints is supported via a Software-as-a-Service (SaaS) platform, known as Entellitrak. Entellitrak is a configurable data tracking and management platform for case management (CM) and business process management (BPM). It provides pre-built, executable business process management system (BPMS) based configurations (process templates) focused on a particular process domain or a vertical industry sector and supports storing data in either an Oracle database or Microsoft structured query language (SQL) server database. iComplaints is accessed via a web-based interface, utilizing a role-based security and access model. The system provides administration and tracking information to the Department.

iComplaints is used to support requirements outlined at 29 CFR § 1614. This regulatory provision requires all Federal agencies to track and report to the Equal Employment Opportunity Commission (EEOC) information concerning the status, processing, and disposition of Federal sector EEO complaints (under Title VII of the Civil Rights Act) so as to adjudicate and issue final decisions and arrive at final disposition of EEO complaints. iComplaints is the Department's system managed by the Office of EEO Services (OEEOS) that provides all the functionality required to collect, track, manage, process, and report on information regarding the processing of the agency's Federal sector EEO complaints and cases.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

Information is collected so that the Department can develop an impartial and appropriate factual record of all Federal sector EEO complaints, including a record of the actions taken during the processing of the complaint. The purpose of this is to adjudicate EEO complaints in a timely manner, order relief if appropriate, and prepare reports mandated by the EEOC.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

New PIA

iComplaints migrated to the Entellitrak SaaS platform, so a new PIA is required.

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Equal Employment Act of 1972, 42 USC 2000e-16, prohibits employment discrimination. The Federal Sector Equal Employment Opportunity Regulations, 29

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

CFR Part 1614, implement the Federal workplace discrimination laws. The Equal Employment Opportunity Management Directive 110 (EEO MD 110) provides Federal agencies with EEOC policies, procedures, and guidance relating to the processing of employment discrimination complaints governed by the EEOC's regulations at 29 CFR. Part 1614.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, 81 FR 81116 (November 17, 2016).

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

GENERAL RECORDS SCHEDULE 2.3, Employee Relations Records, Item 111
EEO Discrimination Complaint Case Files – Formal Process.
Temporary. Destroy 7 years after resolution of case, but longer retention is authorized if required for business use.

GENERAL RECORDS SCHEDULE 5.7, Agency Accountability Records, Item 050
Mandatory Reports to External Federal Entities Regarding Administrative Matters
Temporary. Destroy 6 years after report submission or oversight entity notice of approval, as appropriate, but longer retention is authorized if required for business use.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The PII elements collected are:

- Complainant's name, personal email address, home address, employee pay grade, job series, phone number, date of birth, race, and disability status. Documents submitted by complainant such as charge of discrimination, personal interview statement, and correspondence.

- Employer's name, work phone number, and supervisor's pay plan (if known). Documents submitted by employer such as statement of position, correspondence, statements of witnesses, documentary evidence such as personnel files, records of earnings, employee benefit plans, seniority list, job titles and descriptions, applicant data, organizational charts, collective bargaining agreements, and petitions to revoke or modify subpoenas.

- Information gathered in the course of the investigation and during a hearing, if relevant, such as witness statements, investigator's notes, investigative plan, report of initial and exit interview, investigator's analyses of evidence and charge, subpoenas, decisions and letters of determination, conciliation

agreements, correspondence, and any additional evidence gathered during the course of the investigation.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The system collects the minimum contact information so as to communicate with relevant parties. The additional information collected is the minimum necessary to investigate and adjudicate the complaint.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The individuals who are party to the EEO complaint, the Department, another Federal agency (e.g., EEOC, Merit Systems Protection Board), and EEO Investigators.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The majority of the PII collected is provided by the complainant by completing the EEO Pre-Complaint Intake Form. This form can be submitted electronically through email or provided in hard copy to an EEO specialist. Additional PII mentioned in section 3.1 is compiled through the course of the limited inquiry and investigation.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The PII is validated as it is being collected by either the complainant completing the EEO Pre-Complaint Intake Form and the ongoing communication between the EEO Specialist and the complainant whose information is collected to ensure that updated and accurate PII is being maintained.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

The purpose of the collection is 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 are 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 decisions, and to give complainants adequate and timely notice of their rights. Data may also be used for reporting and statistical purposes, for example Department officials could request the number of complaints filed against a Responsible Management Official (RMO). When used for statistical purposes, personal identifiers will be removed.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The Privacy Act statement provided in 4.2 is part of the package that the EEO specialist provides to the complainant. This PIA and a SORN are also published at www.ed.gov/notices, which provides public notice.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

A Privacy Act statement is provided prior to applicants entering information into the system. Public notices are also provided through this PIA as well as a SORN.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The disclosure of PII is voluntary and individuals who submit a complaint may decline to provide requested information but doing so may result in the dismissal of their complaint because of failure to respond or proceed in a timely fashion.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

Any information collected as part of the complaint process is shared with the Department's Office for Civil Rights (OCR).

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

All data would be shared with OCR for the purpose of litigating the case on behalf of the Department.

External

5.4. Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

The information will be shared with the EEOC pursuant to 29 CFR § 1614.

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

The shared PII is part of an EEO Complaint File (including the EEO Investigative Report). The information is shared with the complainant, and the EEOC via the Federal Sector EEO Portal (FEDSEP). https://egov.eeoc.gov/FedSep/jsp/secure/login.jsf

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

To adjudicate Title VII of the Civil Rights Act, Federal sector EEO complaints.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

Click here to enter text.

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☐ N/A

Information is not disclosed directly from iComplaints. An OEEOS staff member retrieves information from iComplaints and provides it via email, encrypted line, or hard copy.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

No

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

At the conclusion of an EEO Investigation, the complainant is provided with a copy of the report of investigation (ROI). In addition, the complainant can submit a Privacy Act request at any point in the process to obtain their information.

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

The complainant receives a copy of the report of investigation which allows them to correct or update any inaccurate or erroneous information. If an individual wishes to amend the content of a record in the system of records, the individual may contact the system manager according to the instructions in the SORN.

6.3. How does the project notify individuals about the procedures for correcting their information?

Both the SORN and this PIA, as well as the Department's regulations, at 34 CFR 5b7, provide information and procedures for amending records.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

iComplaints is hosted outside of the Department's network on a FedRAMP-certified CSP, Tyler Federal. The system is provided as a SaaS and is required to complete routine testing of their environment to ensure the confidentially, integrity, and availability of the information in the system and services provided. The CSP enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards.

iComplaints utilizes role-based authentication to ensure only authorized users can access information, and they can only access the information needed to perform their duties. Authentication to the server is permitted only over secure, encrypted connections. A firewall is in place which allows only specific trusted connections to access the data. iComplaints has an ATO in place and complies with all National Institute of Standards and Technology (NIST) standards.

Physical safeguards for the data centers are detailed within the system security plan and are assessed as part of the FedRAMP assessment. Tyler Federal does not consume, process, or view the customers' data; no hard copies are made.

MicroPact/Tyler Federal does not access customer production applications without specific approval from the system owner (possibly for troubleshooting purposes). The customer manages application-level access and accounts. Multiple layers of cryptographic mechanisms are in place. There is role-based access control within the application.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

Click here to enter text.

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

The system is currently being assessed by a third party. An initial assessment has been completed by the ISO and Plan of Action and Milestones (POAMs) have been created to address and control deficiencies.

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

MicroPact/Tyler Federal performs monitoring, testing, and evaluation of their software. MicroPact/Tyler Federal is responsible for ensuring access controls are working as defined in the software.

As a part of their continuous monitoring plan, MicroPact/Tyler Federal evaluates and tests a selection of controls internally on a scheduled basis. Assessments are conducted annually by MicroPact/Tyler Federal's third-party organization as part of FedRAMP continuous monitoring requirement; results are reported within the security assessment report. Additionally, MicroPact/Tyler Federal supports multiple customer assessments each year and evaluates those results. Security documentation is reviewed by the information system security officer (ISSO) and the information system owner (ISO) at least annually and updated as required by changes to the system, security posture, or security requirements.

The system production environment has multiple monitoring tools in place. Infrastructure logs are audited. Application-level audit logs can be run by the customer from the administrative module. MicroPact/Tyler Federal also has a continuous monitoring plan in place, which schedules the evaluation/testing of select controls internally. There are a number of reviews conducted by the iComplaints administrator to ensure only authorized users are accessing system data.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures the iComplaints administrator completes reviews of audit logs on a regular basis to ensure there is no misuse or malicious activity with the system or data.

The system owner periodically reviews audit reports provided by the iComplaints administrator regarding information processing and maintains the access control list for who can read/write any PII. The ISO also works directly with the Department's privacy office on privacy compliance documentation to ensure all information in this PIA is up to date and accurate. Ultimately, the iComplaints system application(s) undergo yearly OMB Circular A-123, Appendix A (Management's Responsibility for Enterprise Risk Management and Internal Control) assessment, and NIST Special Publication 800-53 system security control self-assessments.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. To address privacy risks, iComplaints has several mitigations in place. For example, iComplaints has an agreement of OFO Rules of Behavior by system users and an account approval process to provide role-based accounts which limit the read/write capability of the user. The main privacy risk identified is unauthorized access to the PII contained in the iComplaints application. The risk has been mitigated through privacy training for both contractors and Department staff, restricting access to PII to those individuals with a direct business need for the information, and robust security controls such as the use of firewalls, intrusion detection systems, and event monitoring systems provided by the applications CSP.