Privacy Impact Assessment (PIA)

for the

ADR CTS-Alternative Dispute Resolution Center Case Tracking System

May 10, 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: David Wortham
Contact Email: David.Wortham@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 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).

The Alternative Dispute Resolution (ADR) Center is a forum for informal problem resolution before there is a need for an employee to file a formal grievance or complaint. If an employee has any complaint concerning any matter related to their employment, the employee is authorized to have the complaint addressed informally by the ADR Center.

The ADR Center Case Tracking System (ADR CTS) is a web-based application that is platform-independent of other user operating systems (i.e., iOS, Windows). ADR CTS 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. ADR CTS 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.

The purpose of the ADR CTS is to collect, use, maintain, and review information related to informal grievances (administrative and negotiated) and Equal Employment Opportunity (EEO) complaint referrals. To properly manage cases, the ADR Center ensures that the ADR Center Intake Form that is provided by the employee is complete and loaded to into the ADR CTS.

In addition to storing case information, the ADR CTS tracks metrics on the total number of ADR Center contacts and provides reporting statistics on the timeliness of case processing. The system manages case timeliness to ensure regulatory compliance with established deadlines. In addition to tracking the timeliness of each case, the ADR CTS identifies the specific ADR technique (mediation, facilitation, and conflict coaching) employees and applicants elect to use during the ADR Center process.

The ADR CTS also identifies and tracks all participants in the ADR process, using an automatically assigned tracking number. Quarterly, the ADR CTS generates reports that analyze the overall operation of the ADR Center process. A typical ADR CTS report identifies the total number of informal grievances (administrative and negotiated) and Equal Employment Opportunity (EEO) complaint referrals, provides data on the number of cases assigned to each ADR Center staff member, provides the status of those cases (open or closed) assigned, provides the location (headquarters or regional office) of the employee or applicant, and provides the ADR technique used for each assigned case. These reports are provided to the Department's senior management officials.

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

Information maintained on the ADR CTS is used for several purposes. Information collected through the ADR CTS Intake Form and during the investigation into the complaint is collected to support the informal grievance and complaint resolution process prior to proceeding to the Department's formal grievance and complaint processes. Once information is collected and verified by the ADR analyst, the analyst determines which formal Department process would be followed to resolve the grievance. The ADR CTS system is also used to generate reports for senior officials to provide visibility into the status of disputes at the Department.

The ADR Center also uses the collected PII to identify and contact case participants. An automatically generated tracking number is used to track ADR Center cases.

[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

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

ADR 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 ADR Center's jurisdiction is limited to matters referred to the office pursuant to statute, regulation, directive, or other internal policy document. The current list of authorities is listed below:

1. Title VII of the Civil Rights Act of 1964
2. The Equal Pay Act of 1963
3. The Age Discrimination in Employment Act of 1967
4. Titles I and V of the Americans with Disabilities Act of 1990 (ADA)
5. Personnel Manual Instructions (PMI) 771-1 Employee Grievances
6. Collective Bargaining Agreement, March 12, 2018

These authorities allow for employees and applicants to informally resolve a wide range of employment disputes, disagreements, or complaints on work-related matters, such as grievances and EEO complaints.

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

The system of records entitled "Alternative Dispute Resolution (ADR) Center Case Tracking System" (18-05-12) was published in the Federal Register on June 4, 1999 (64 FR 30137-30139) and most recently amended on November 9, 2011 (77 FR 67349-67352).

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.

GENERAL RECORDS SCHEDULE 2.3: Employee Relations Records
Temporary. Destroy 3 years after case is closed, but longer disposition 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?

[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

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 ADR Center Intake Form collects the following required information:

- Names and preferred contact method of case participants. This contact information would include telephone numbers, email addresses, and work location.
- Summary of issues surrounding the case.
- The date the ADR Center was contacted.
- The client type:
  - EEO Formal - Employee/applicant case at formal stage of EEO process.
  - EEO Informal - Employee/applicant case at pre-complaint stage of EEO process.
  - Educational Outreach – Employee seeking some sort of conflict resolution training.
  - Inquiry – Employee/applicant seeking information or advice.
  - Pre-Administrative Grievance – Employee is a non-bargaining unit employee.
  - Pre-Negotiated Grievance – Employee is bargaining unit employee.
  - Unknown - Employee/applicant does not fit any of the categories above.
- The name and contact information of the assigned ADR analyst.
- How the client heard about the ADR Center.

Additional information could be provided by the client. Examples of additional information provided by clients would be letters of reprimand or performance evaluation results. In addition to the elements collected as part of the ADR CTS Intake Form, the ADR CTS contains various types of PII, depending on the case. The ADR CTS Intake Form could also include the PII of individuals other than the complainant who are associated with the case within the summary of issues statement.

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

Yes

ADR CTS collects only the minimum information necessary to administer the program. Contact information is needed to communicate with the parties and conduct the informal grievance and complaint resolution process. In addition, certain case files are maintained to ensure proper record keeping. No information is collected that is not required to achieve this purpose.

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

ADR CTS PII sources come from clients participating in the ADR Center process.

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 ADR Center staff member assigned a new case collects PII from the client initially via paper or electronic format via the Intake Form. Database collection is from all electronic and paper sources submitted. The PII is manually entered into the ADR CTS by the ADR Center staff member assigned to the case.

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 client validates PII when they complete and sign the paper or electronic copy of the ADR Center Intake Form. The personal contact information is again validated by the client each time the client requests to use alternate contact information. The PII submitted to the application has been vetted by the Department's Human Resources office at the time of hiring. If the participant provides incorrect information, they will not receive expected communications and will likely reach out to the ADR Center to provide the correct information.

Use

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

The ADR Center uses the PII described above to contact clients of the ADR Center process. In addition, the information is collected to support the informal grievance and complaint resolution process prior to proceeding to the Department formal grievance and complaint processes. Once information is collected and verified by the ADR analyst, the

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

analyst determines which formal Department process would be followed to resolve the grievance.

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.

A Privacy Act statement is provided to users on the Intake Form prior to them entering information into the system. When employees or applicants receive an Intake Form to complete, they must sign and date the Intake Form indicating they are aware some PII will be collected and the PII provided is correct. 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

Click here to enter text.

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?

Clients are asked to provide their PII on the ADR Center Intake Form. If the client does not provide the PII or does not sign the Intake Form, the PII is not collected and entered into the ADR CTS. While using the ADR process is voluntary, providing PII is mandatory to follow the process.

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

The information could be shared with the Department's General Counsel, Human Resources, Labor Resources, Labor Relations, Employee Relation, Equal Employment Opportunity Service, and Federal Student Aid offices.

5.2. What PII will be shared and with whom?

☐ N/A

The same PII listed within section 1.2 could be shared with the offices identified in section 5.1.

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

☐ N/A

The information is shared with those offices to support the informal grievance and complaint resolution process prior to proceeding to the Department's formal grievance and complaint processes. Once information is collected and verified by the ADR analyst, the analyst determines which formal Department process would be followed to resolve the grievance.

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.

No

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

[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.

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

☑ N/A

Click here to select.

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

☑ N/A

Click here to enter text.

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

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

If an individual wishes to determine whether a record exists about the individual in the system of records, the individual may contact the system manager. The request process is described in the system of records notice. Requests must meet the requirements in the Department's regulations at 34 CFR 5b.5, including proof of identity.

If an individual wishes to gain access to a record in this system, the individual may contact the system manager. The request process is described in the system of records notice. Requests by an individual for access to a record must meet the requirements in the Department's regulations at 34 CFR 5b.5, including proof of identity.

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

If an individual wishes to contest the content of a record in the system of records, the individual may contact the system manager. The request must meet the requirements of the Department's regulations at 34 CFR 5b.7, including proof of identity.

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 correcting inaccurate information.

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

This system is one of the six MicroPact/Tyler Federal systems contained within the Electronic Case Management Processing (ECAMP) system, which is in the process of getting an authorization to operate (ATO).

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?

ADR CTS 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.

ADR CTS 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. ADR CTS 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

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

Yes

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.

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 ADR 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 ADR 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 ADR CTS 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.

The ADR CTS has several privacy risk mitigation strategies in place. For example, there is a requirement for employees that utilize this application to have a position risk designation of either moderate or high risk, an active Department account, and a signed Office of Finance and Operations Rules of Behavior. For additional information on the Department's Federal Employee Personnel Security Screenings Process, please refer to OFO: 5-102. The main privacy risk identified is potential unauthorized access to the PII contained in ADR CTS. The risk has been mitigated through privacy training for both contractor(s) and Department staff, restricting access to PII to those individuals with a direct business need for the information, and robust security and privacy controls such as through the use of firewalls, intrusion detection systems, and event monitoring systems.