Privacy Impact Assessment (PIA)

for the

OHA CTS -- Office of Hearings and Appeals E-Filing System

June 2, 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: George Abbott
Contact Email: george.abbott@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).

The Office of Hearings and Appeals E-Filing System (OHA CTS) is a web-based application that is platform-independent of other user operating systems (i.e., iOS, Windows). OHA 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. OHA 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.

OHA CTS is the online filing system for all matters before OHA. When matters are appealed to OHA, an electronic case file is created in OHA CTS. All pleadings, exhibits, and other documents filed with OHA become attached to the electronic case file. The use of OHA CTS is not mandatory as by federal regulation the Department cannot require a respondent to file electronically, however OHA opens an OHA CTS case file for all matters, regardless of whether e-filing is used. As of January 1, 2019, OHA CTS is the official file for all OHA CTS matters.

Matters before OHA CTS include, but are not limited to, disputes between the Department and financial assistance recipients (schools, school districts, a state's

education department, students, etc.), certain debarment actions, and disputes between the Department and current or former employees regarding salary overpayment(s).

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

OHA CTS contains various types of PII, depending on the case, for adjudicatory purposes. The documents containing PII in OHA CTS are submitted by the parties to allow the court to consider evidence in rendering a decision. The information is collected to adjudicate requests for waivers of salary overpayments and claims regarding the validity of salary overpayments made to current and former employees and to adjudicate administrative wage garnishments. The Department also uses the OHA CTS to provide docket management, including scheduling of hearings, oral arguments, and determining compliance with parties' filing deadlines and to produce docket reports that may be distributed internally in the Department.

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

OHA CTS 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

[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

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.

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

- General Education Provisions Act, as amended by Public Law 100-297
- Sections 5(d)(2)(A) and 5(g) of the Impact Aid Act (Public Law 81-874)
- Title VI of the Civil Rights Act of 1964, as amended
- Title IX of the Education Amendments of 1972, as amended
- Section 504 of the Rehabilitation Act of 1973, as amended
- Age Discrimination Act of 1975, as amended
- Program Fraud Civil Remedies Act, as amended, Public Law 99-509, Title VI, subtitle B
- Civil penalty proceedings under section 432(g) of the Higher Education Act of 1965, as amended (HEA), 20 U.S.C. 1082(g)
- Review proceedings under section 432(h)(2) of the HEA, 20 U.S.C. 1082(h)(2)
- Review proceedings under section 432(h)(3) of the HEA, 20 U.S.C. 1082(h)(3)
- Proceedings under section 487(b) of the HEA, 20 U.S.C. 1094(b)
- Proceedings under section 20 U.S.C. 1094(c)(1)(F) and 20 U.S.C. 1094(c)(3)(A)
- 5 U.S.C. 5584; 31 U.S.C. § 3711 et seq.
- 34 CFR part 32
- 34 CFR part 34
- Federal Claims Collection Standards (FCCS) 31 CFR chapter IX, parts 900–904

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.

The Office of Hearings & Appeals (OHA) Records System, 18-05-19, 78 FR 62605 (October 22, 2013).

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.

Department Schedule 243, *Decisions Made by Hearing Officials, Administrative Law Judges, the Secretary of Education, and Members of CRRA*

PERMANENT Remove original decision before official docket file is transferred to a certified records center. Hold on site and transfer to the National Archives in five-year blocks. Schedule 241, *Administrative Adjudication Case Files for the Office of Hearings and Appeals.*

TEMPORARY Cut off annually upon close of case. Transfer to a certified records center or to a certified records storage facility 1 year after cut-off. Destroy/delete 6 years after cutoff.

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 specific PII varies by type of case. The below list is not exhaustive, but these items are somewhat common in OHA cases.

- Name (students and sometimes parents)
- SSN (generally only last 4 digits)
- Address
- Email address
- Telephone number
- Student ID number (generally a number created for litigation, not the true student ID number)
- Payroll information
- Employee's personnel records
- Taxpayer ID and tax transcripts
- Banking and/or financial account records, numbers, or information
- Federal/state criminal/civil court records
- Medical records
- Salary information (for overpayment cases)

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

Yes, the OHA CTS system collects only the minimum required information to facilitate the adjudication process to be consistent with the Federal rules, regulations, and statues.

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

All information in OHA CTS comes from the litigants.

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

Parties submit their information by uploading it OHA CTS.

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?

OHA does not validate or confirm the information, rather it relies on the opposing party to do any validation. For example, if a school submitted information that the Department challenged, Department attorney(s) would review the document in question and note their objections for the record.

Use

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

The hearing official reviews the information to analyze the matter and render a decision. The information becomes part of the official administrative record if the matter is appealed to the Secretary or a Federal court.

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 (SSN), 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.

[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.

Yes

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

☑ N/A

OHA CTS does not request SSNs from parties and the assigned Judge provides the order of governing proceedings which includes instructions for parties to not include social security numbers within information provided. However, OHA allows parties to submit evidence that may include SSNs if the parties choose to provide them. The parties sometimes submit SSNs to establish matters relevant to the case in question. For example, a school will sometime submit SSNs for students it contends attended the school, and employees will sometimes submit pay/personnel documentation to support their waiver request.

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

☐ N/A

OHA considered redacting all SSNs but concluded that SSNs are necessary for adjudication in many cases. Instead OHA has elected to minimize the presence of SSNs by directing the parties, particularly in Federal Student Aid (FSA) disputes, to redact all PII with the exception of name and last 4 digits of SSN. Redaction of all PII is infeasible as the documentation can be voluminous and can be comprised of large packages of poorly copied/hand-written documents.

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.

OHA CTS does not provide direct notice because OHA does not typically collect PII from individuals. Instead, parties who wish to submit evidence (which may include PII), upload it into OHA CTS. The OHA webpage provides public notice regarding the submission of PII to OHA CTS.

Some of the information originates in other Departmental systems, such as FSA systems that process student financial assistance information. Individual users of those other systems receive privacy notice when they upload their PII. The majority of PII in OHA CTS comes from a process in which OHA is not a party and therefore OHA is unable to

notify the individual/entity submitting PII to the program office of OHA's inheritance of PII.

For the salary overpayment cases, the individual seeking redress will sometimes submit PII if they believe it will help their case, but PII is not required.
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

www.oha.ed.gov

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?

Most system users are external entities, such as schools and state agencies. These entities can elect to submit or not submit PII to the program office. OHA places in OHA CTS what the entity has elected to submit to program office. Individual employees of the Department may elect to use OHA CTS for salary overpayment matters.

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 it is reviewed at the same frequency of PIA reviews.

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

When cases are appealed to Federal court, the administrative record, including evidence, is reviewed by the Office of the General Counsel (OGC) prior to submittal.

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

☐ N/A

When cases are appealed to Federal court, the administrative record, including evidence, is reviewed by OGC prior to submittal for the purpose of ensuring PII is not within the documents.

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

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

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

☑ N/A

[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.

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

☑ N/A

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

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

☑ N/A

6. Redress

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

If you wish to contest the content of a record regarding you in the system of records, contact the system manager. Your request must meet the requirements of the regulations at 34 CFR 5b.7.

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

As documented in the OHA CTS SORN, if you wish to contest the content of a record regarding you in the system of records, contact the system manager. Your request must meet the requirements of the regulations at 34 CFR 5b.7. .

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

The Hearing Official issues an Order Governing Proceedings in each matter that informs litigants, including individuals, how to file documents with the court.

Additionally, 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

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?

OHA 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.

OHA 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.

OHA 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

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 OHA CTS 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?

In OHA CTS, each case file contains a list of authorized users. The authorized user assigned list is reviewed by the hearing official and the administrator for any access discrepancies. A user that is not listed in the case assignment list cannot access that particular case. A party wishing to have access to a case must file a Notice of Appearance with OHA. That notice is reviewed by the Hearing Official assigned to the requested case. The Hearing Official will make a determination if case access is to be granted to a requesting party.

The system owner ensures the OHA CTS 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 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 OHA CTS system applications 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. The privacy risks are mitigated through data minimization and generally requiring parties to redact PII except for name and the last four digits of the SSN. Additionally, the controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additional mitigations include an agreement to 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.

Unauthorized access to the PII contained in the OHA CTS application is also a risk. This 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-related controls such as through the use of firewalls, intrusion detection systems, and event monitoring systems provided by the application's CSP.