Privacy Impact Assessment (PIA)

for the

Alternative Dispute Resolution Center Case Tracking System (ADR CTS)

March 27, 2024

Point of Contact

Contact Person: David Wortham
Title: ADR Analyst
Email: David.Wortham@ed.gov

System Owner

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

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

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

Electronic Case Management Platform (ECAMP) is an integrated U.S. Department of Education (Department) system that utilizes the Entellitrak and iComplaints software-as a-service (SaaS) solutions provided by Tyler Technologies. The Entellitrak and iComplaints solutions are enterprise-level commercial off-the-shelf (COTS) products that provide all functionality required to collect, track, manage, process, and report on information regarding several Department business initiatives within the Office of Finance and Operations (OFO).

1.2. How does the IT system function to support the project or program as described in Question 1.1?

Alternative Dispute Resolution Center Case Tracking System (ADR CTS) is hosted outside of the Department's network by a FedRAMP-certified cloud service provider (CSP), Tyler Technologies. The system is provided as a SaaS and Tyler Technologies does not consume, process, or view the customers' data, and no hard copies are made. ADR CTS is an ECAMP web-based application used for processing informal employment complaints before a need for filing a formal grievance or complaint arises. ADR CTS collects information related to informal grievances and complaints via the Alternative Dispute Resolution (ADR) Center Intake Form, which is loaded into the system. ADR CTS identifies and tracks all participants in the ADR process using an automatically assigned tracking number. ADR CTS generates quarterly reports analyzing the overall operation of the ADR process, including the total number of informal grievances and complaints, the number and status of cases assigned to each ADR Center staff member, the office location of the employee or applicant, and the ADR method used for each assigned case.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☐ Portal	☒ Application
☐ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

Information maintained within ADR CTS is used for several purposes. Information collected through the ADR CTS Intake Form 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 within OFO's ADR Center, the analyst determines which 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 uses the collected PII to identify and contact case participants. An automatically generated tracking number is used to track ADR Center cases.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☐ N/A

[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

ADR CTS is a COTS SaaS product supported by Tyler Technologies as the CSP. Tyler Technologies is responsible for maintaining, patching, and updating both the system and the server it resides on.

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

Yes

☐ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The ADR Center's jurisdiction is governed by statute, regulation, directive, and 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)

These authorities allow for employees and applicants to seek resolution on a wide range of employment disputes, disagreements, or complaints on work-related matters.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being

prepared.

The SORN, titled "Alternative Dispute Resolution (ADR) Center Case Tracking System," 18-05-12, 77 FR 67348, was published in the Federal Register on November 8, 2012.

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information.
List the schedule(s):

Disposition for ADR CTS files is covered by General Records Schedule 2.3, "Employee Relation Records," item 070:

070	**Alternative Dispute Resolution (ADR) case files.** Includes: • agreements to use ADR • records of intake and process • records of settlement or discontinuance of case • parties' written evaluations of the process	**Informal process.** Records not associated with another employee dispute, complaint or grievance process.	**Temporary**. Destroy 3 years after case is closed, but longer disposition is authorized if required for business use.	DAA-GRS-2018-0002-0007

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☐ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☒ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☒ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII:

The ADR Center Intake Form collects the following required information:

- Names and preferred contact method of case participants. This contact information includes preferred telephone numbers, email addresses, and work location.

- Summary of issues surrounding the case.
- The date the ADR Center was contacted.
- The client/participant type (how the participants are categorized based on how the ADR Center will handle the case):
  - 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 office contact information of the assigned ADR analyst.
- Information about how the client/participant heard about the ADR Center.

Additional information could be provided by the participant in support of their claim. Examples of additional information provided by participants 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. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Name, preferred phone number, preferred email address, and work location of case participants; summary of issues surrounding the case; date the ADR Center was contacted; case number; and name, phone number, email address, and work location of the ADR analyst assigned to case.

Name, phone number, email address, and work location of other individuals associated with the case, as well as other information, such as letters of reprimand or performance evaluation results, could also be collected if required.

Username and passwords are also collected from Department employees who have access to the system for the purpose of administering accounts.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Username and passwords are collected for the purpose of administering accounts.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

The following could be collected from applicants for employment or former employees:
Name, preferred phone number, preferred email address, and work location of case participants; summary of issues surrounding case; date the ADR center was contacted; and case number, name, phone number, email address, and work location of other individuals associated with the case, as well as other information, such as letters of reprimand or performance evaluation results, could also be collected if required.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

The PII comes directly from individuals participating in the ADR informal grievance and complaint resolution process. Participants can include individuals who filed a complaint, as well as other participants in the process.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

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

The ADR Center staff member assigned to a case initially collects PII from the participant via paper or electronic format on the above-mentioned Intake Form. The PII is then manually entered into the ADR CTS by the ADR Center staff member assigned to the case. Participants do not enter information directly into ADR CTS.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

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.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees
☒ Federal Contractors
☐ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

The participant 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 participant each time the participant requests to use alternate contact information. If the participant is an employee, the PII submitted will have 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. Details about the complaint submitted will be reviewed as part of the informal complaint resolution stage.

If the complaint proceeds to the formal resolution process, the details about the complaint are validated within a separate system.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

No

The Department does not actively collect SSNs, however, complainants may provide them in the submission of evidence. Submitting SSNs is not required.

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☑ N/A

3.9.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☑ N/A

3.10.3. If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☒ N/A

3.10.4. If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☑ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A Privacy Act Statement is provided on the ADR Intake Form prior to any PII submission.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

Yes

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

Below is the Privacy Act Statement on the ADR CTS Intake Form:

Authorities: The following list of authorities that authorize the collection of this information:

- Title VII of the Civil Rights Act of 1964
- The Equal Pay Act of 1963
- The Age Discrimination in Employment Act of 1967
- Titles I and V of the Americans with Disabilities Act of 1990 (ADA)

- Personnel Manual Instructions (PMI) 771-1 Employee Grievances
- Collective Bargaining Agreement, March 12, 2018

The collection of SSNs of users of this system is also authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

Purpose: The purpose of collecting this information is to use and review information related to informal grievances (Administrative and Negotiated) and Equal Employment Opportunity (EEO) complaint referrals, in order to make a determination regarding the complaint.

Routine Uses: In addition to those disclosures permitted under 5 U.S.C.552a(b) of the Privacy Act, information contained in this system may be disclosed outside of ED as a routine use pursuant to 5 U.S.C. 552a(b)(3) when the disclosure is compatible with the purpose for which the records were compiled. The routine use disclosures are detailed in the system of records titled Alternative Dispute Resolution (ADR) Center Case Tracking System.

Consequences of Failure to Provide information: Furnishing this information is voluntary; however, failure to provide the information requested may prevent ED from processing your compliant.

SSN Use: The Department does not actively collect SSNs, however, complainants may provide them in the submission of evidence. Submitting SSNs is not required.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Participants are asked to provide their PII on the ADR Center Intake Form. If the participant does not provide the PII or does not sign the Intake Form, the PII is not collected and is therefore not entered into the ADR CTS. While using the ADR process is voluntary, providing PII is mandatory in order to participate in the process.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

The PII listed within section 3.1 could be shared with the Department's General Counsel, Human Resources, Labor Resources, Labor Relations, Employee Relations, Equal Employment Opportunity Service, and the affected principal office as well as an ADR Center participant representative (legal or otherwise).

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

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

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

Information from ADR CTS may be shared with external entities pursuant to the routine uses listed in the SORN for ADR CTS. Information may be shared with other entities without the consent of the individual if the routine use disclosure is compatible with the

purposes for which the record was collected. Please refer to the SORN listed in question 2.2.1 for a comprehensive list of routine uses.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

Information from ADR CTS may be shared with external entities pursuant to the routine uses listed in the SORN for ADR CTS. This sharing is related to the informal grievance and complaint resolution process. For example, The Department may disclose a record to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to a Department decision concerning the hiring or retention of an employee or other personnel action.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

The current list of authorities are listed below:

- Title VII of the Civil Rights Act of 1964
- The Equal Pay Act of 1963
- The Age Discrimination in Employment Act of 1967
- Titles I and V of the Americans with Disabilities Act of 1990 (ADA)

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

Information is shared in a secure fashion normally through various secure encrypted file sharing applications, depending on the security requirements of the Department and the recipients.

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

☐ N/A

No

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

If an individual wishes to gain access to a record in this system, they may contact the system manager listed in the SORN above in question 2.3. Requests by an individual for access to a record must meet the requirements the regulations at 34 CFR 5b.5, including proof of identity.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

If an individual wishes to contest the content of a record regarding themselves in this system of records, they may contact the system manager listed in the SORN above in question 2.3. Your request must meet the requirements of the Act regulations at 34 CFR 5b.7, including proof of identity.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Both the SORN and this PIA, as well as the regulations found in 34 CFR 5b.7, under which the Department operates, 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 ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐ Low

☒ Moderate

☐ High

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 Technologies. 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. As stated above, Tyler Technologies does not consume, process, or view the customers' data; no hard copies are made.

Tyler Technolgies 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.

8. Auditing and Accountability

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

The ADR CTS system application undergoes yearly Office of Management and Budget 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. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

The system owner ensures the ADR CTS Administrator completes reviews of audit logs on a quarterly basis to ensure there is no misuse or malicious activity with the system. The system owner reviews the audit logs provided by the ADR CTS Administrator regarding information processing and maintains the access control list for who can read/write any PII. The system owner also works directly with the Department's Privacy Program on privacy compliance documentation to ensure all information in this PIA is up to date and accurate.

ADR CTS, as part of the ECAMP application, is required to obtain and maintain an ATO. This process includes an independent assessment of all required security and privacy controls and produces plans of action and milestones (POA&Ms) to ensure any deficiencies are remediated. ECAMP will also participate in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews Federal Information Security Modernization Act controls, is conducted quarterly, and the system is scanned continuously to ensure that security and privacy controls are in place and working properly.

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

The main privacy risks include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs. The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks. In addition, the risks have 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 using firewalls, intrusion detection systems, and event monitoring systems. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. There is a requirement for employees that utilize this application to have a position risk designation of either moderate or high risk (requiring that the employee undergo a screening process), an active Department account, and agree to the Office of Finance and Operation's Rules of Behavior.