Privacy Impact Assessment (PIA)

for the

Case Management Tracking System (CMTS)

February 13, 2023

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: Frank E. Miller Jr./Deputy Director, Student Privacy Policy Office (SPPO)
Contact Email: Frank.E.Miller@ed.gov

System Owner

Name/Title: Frank E. Miller Jr./Deputy Director, SPPO
Principal Office: Office of Planning, Evaluation, and Policy Development

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 Case Management Tracking System (CMTS) supports the Student Privacy Policy Office (SPPO) at the U.S. Department of Education (Department) by managing and tracking SPPO's workflow processes. The CMTS updates and expands the contractor-operated application that SPPO uses to track the resolution of informal requests for technical assistance from stakeholders to also track the submission of complaints and other enforcement actions under the Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA), and the submission of information security incidents from certain educational institutions. The CMTS will include four components:

- Public web portal – A public-facing webpage where external users, those outside the Department, will be able to create a user profile to log in and submit a FERPA or PPRA complaint, upload documentation in support of the complaint, and check the status of the complaint. The web portal will also allow educational agencies and institutions that are the subject of such complaints or an investigation self-initiated by SPPO, to upload supporting documentation requested by SPPO. Note: as further discussed below, technical assistance requests will continue to be submitted via webform on the existing website or by telephone or email.
- Case Management System (CMS) – A system built using a COTS Customer Relationship Manager (CRM) product called Agiloft that will track SPPO's enforcement activities. Complainants will be able to create an account and log their complaint into the CMTS. Upon receipt, the triage team will either dismiss the complaint or assign the complaint to a caseworker for further enforcement action. During this action, the caseworker will be able to prompt both the complainant as well as the school for additional information, which may be uploaded directly into the system. The system will use customized business rules and agents that will automate many aspects of the investigation process. In the case of a self-initiated investigation, SPPO will be able to create a case in the system to track the workflow of the investigation and function in the same way as a complaint.

- CMS tools and administration – Back-end administrative functions that allow for the customization of the CMS.
- Back-end database – A relational database where the information collected by the CMTS is stored.

The CMTS processes and tracks:

- Student privacy complaints and other enforcement actions under FERPA and PPRA.
- Informal requests for technical assistance on student privacy matters from stakeholders across the Department and the public.
- Self-initiated actions by SPPO.

CMTS facilitates SPPO's tracking of complaints, other enforcement actions, and technical assistance requests related to Federal student privacy laws. Complaints are submitted to the Department by individuals who are alleging violations of one or both privacy laws that SPPO administers, FERPA and PPRA. Complaints are initiated by a member of the public and managed by an SPPO caseworker. The system collects identifying information from the complainant, information about the alleged violation, the name of the institution that may have violated the law, the names of institution administration/staff, the names and information about witnesses or other parties to the complaint, as well as information about the investigation and final resolution of the complaint. Technical assistance requests are informal inquiries from parents, school officials, attorneys, and other stakeholders about student privacy and information security. Data collected for technical assistance inquiries will include name, address, and phone number of the requestor, as well as the details of the question and the response provided by SPPO. SPPO can also initiate an enforcement or technical assistance action without receiving a complaint or request from a complainant or other stakeholder; the system may collect similar information for these cases.

Historically, complaints and correspondence were submitted to SPPO in paper form or electronically via email. SPPO plans to use the CMTS to allow complainants and technical assistance requestors to choose to submit information through an electronic form on our website at https://studentprivacy.ed.gov/, as well as the aforementioned methods of submission. The CMTS will allow complainants to create user accounts to submit a complaint, as well as documentation to support that complaint, or as requested by SPPO to provide additional information about an enforcement action. In addition, where SPPO takes an enforcement action in response to a complaint, or self-initiates such action in the absence of a complainant, the educational agency or institution subject to that enforcement may also create a user account to submit a written response to the

allegations or provide other information as requested by SPPO. While the submission of a complaint will require user registration, account creation is not required for the submission of technical assistance inquiries. Technical assistance requests will continue to be submitted via webform on the existing website or by telephone or email.

ICAM (Identity, Credential, and Access Management) has been chosen to be implemented as an authentication method to provide secure and efficient access control for the organization's systems and resources. ICAM will enable the organization to manage the lifecycle of digital identities, ensuring that the right people have the right access to the right resources, while also providing protection against unauthorized access. The implementation of ICAM will help to ensure the confidentiality, integrity, and availability of critical information and systems, as well as comply with government regulations, requirements, and standards.

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

PII collected and maintained by this system is used to obtain and resolve complaints alleging violations of FERPA and PPRA, conduct other student privacy enforcement actions, as well as address informal requests for technical assistance on student privacy matters from stakeholders. PII will also be used to create reports to analyze and support SPPO's operations.

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

New System

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

New PIA

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?

[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

☐ 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.

Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 CFR part 99), Protection of Pupil Rights Amendment (20 U.S.C. 1232h and 34 CFR part 98).

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

"Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendments (PPRA) Records Systems," 18-05-02, June 4, 1999.

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

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] 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

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.

Records in this system are retained and disposed of in accordance with:

- Department Records Schedule ED 162, "Family Policy Compliance Office Complaints and Technical Assistance" (N1-441-09-18)
- General Records Schedule 3.2, "Information Systems Security Records" (DAA-GRS-2013-0006-0001)
- General Records Schedule 4.2, "Information Access and Protection Records" (DAA-GRS-2016-0003-0003) and (DAA-GRS-2016-0003-0004).

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.

This system maintains information about complaints from parents and eligible students alleging violations of FERPA or PPRA, information about other enforcement actions under these laws, e.g., information regarding those actions self-initiated by SPPO, as well as requests for technical assistance from members of the public on student privacy matters. This information may include requestor's first and last names, addresses, phone numbers, dates of birth, email addresses, details about the person's complaint or inquiry, and any additional details provided as part of the complaint, enforcement action, or inquiry. The information may also include names, contact information, job title, and other information from school officials, Local Education Agency (LEA) officials, state education agency officials, witnesses, attorneys, advocates, or other individuals who are involved in an enforcement action. Additional PII may be obtained on a case-by-case basis via correspondence during the investigative process, including but not limited to items such as transcripts or other academic records, medical records, disciplinary records, and letter and/or email exchanges between parents/students and an educational institution. SPPO never requests Social Security numbers (SSN); however, there are times when a complainant or requestor includes them when submitting supplemental information. In these cases, the intake specialist will redact or delete the SSN, as appropriate.

FERPA and PPRA Complaint Forms collect the following PII:

- Student first and last name
- Student date of birth
- Complainant first and last name
- Complainant address
- Complainant email address
- School official or LEA point of contact name and contact information
- Details about the complaint
- Signature of complainant

Informal requests for technical assistance collect the following PII:

- Requestor first and last name
- Requestor phone number
- Requestor email address
- Details about the request

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

Yes

The CMTS collects the minimum amount of PII required to track the resolution of the informal requests for technical assistance, the submission of complaints regarding FERPA and PPRA, the resolution of other enforcement actions under those laws, and the submission of reports of information security incidents or breaches from educational institutions. PII is also required to provide support for informal requests for technical assistance from stakeholders across the Department and the public. Information accessed through CMTS is needed to address any questions or issues posed by the public or Department personnel. If the PII was not provided, the Department may not be able to process and resolve the complaint, enforcement action, or request for technical assistance.

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

The information collected for FERPA and PPRA enforcement is collected directly from the complainant (a parent or eligible student) or from an attorney/advocate on their

behalf through an approved information collection form and through back-and-forth communication with the parties to a complaint. Following receipt of the complaint or initiation of an enforcement action, information will also be collected from the representative of the educational agency or institution that is alleged to have violated FERPA or PPRA and is subject to the enforcement action. As part of an investigation SPPO may also consult with and obtain information from other entities such as the U.S. Department of Justice, another Department office such as the Office for Civil Rights, law enforcement entities, and state education agencies. The information collected for technical assistance requests is collected directly from the person or entity that is requesting technical assistance and from any other party to the request.

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 CMTS will use a web form via the web portal discuss that collects the same data points as found on the Office of Management and Budget (OMB) approved FERPA and PPRA complaint forms. The complainant will also have the ability to upload supplemental documentation in support of their complaint. In addition, upon notification of our initiation of an enforcement action, whether in response to complaint or as part of a self-initiated action by SPPO, the educational agency/institution that is the subject of the action will be able to access the web portal discussed above in Section 1.1, and create a profile that can be used to upload documentation as requested by SPPO to be incorporated into the case record for that specific action. Complainants who do not wish to use the web form, may continue to submit their complaints using the PDF version of OMB approved complaint forms as posted on our website and sending to SPPO through email, or in hard copy paper form submitted through the U.S. Postal Service. Complaints submitted using these methods will be transcribed into the system by staff who will be responsible for coordinating subsequent document submission and data entry. Informal requests for technical assistance can be submitted through the webpage, or if submitted via email, letter, or phone call, the request will be manually transcribed by the intake staff person, help desk staff, or case worker that is fielding the call, email, or letter. Over the course of an enforcement action, case workers may need to collect additional information which can be gathered through the CMTS, through phone call, email, or by letter.

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?

[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.

Information provided to the CMTS is provided by a parent, eligible student, Department personnel, or education agency. While the system has required fields, audit logs, and validation rules, it is ultimately the responsibility of the user to provide valid and accurate information. All information collected during the course of an enforcement action will be verified by SPPO caseworkers to, first, determine its relevancy to the action, and second, determine the authenticity and veracity of the information, to the extent possible, during the course of an investigation. SPPO has the regulatory authority to request additional clarification as needed to make these determinations, and ultimately weighs the merits of this information in determining how to effectively resolve the enforcement action. All parties to an enforcement action and technical assistance requestors are able to contact SPPO to correct or amend any information previously submitted through the same channels through which they provided the information.

Use

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

PII maintained in this system is used to determine whether the complaint: is filed by an individual who maintains FERPA or PPRA rights over the education records which are the subject of the complaint; is submitted to the Department within 180 days of the date of the alleged violation or of the date that the complainant knew or reasonably should have known of the alleged violation; and contains specific allegations of fact giving reasonable cause to believe that a violation of FERPA or PPRA has occurred. If those conditions are met, the information in the system is then used to investigate alleged violations of FERPA and PPRA and reach a determination.

In addition, SPPO has the authority to conduct its own enforcement action when no complaint has been filed, when the complaint has been withdrawn or is not filed by an individual who has standing to file such complaint, as long as there are specific allegations of fact giving SPPO reasonable cause to believe that a violation of FERPA or PPRA may have occurred. In such cases, the information in the system is used to investigate alleged violations of FERPA and PPRA and reach a determination.

With regard to general technical assistance inquiries, requests for policy clarification, and reports of data breaches, the information will be used to analyze and respond to the request, as appropriate.

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

Social Security Numbers

It is the Department's Policy that, 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

Social Security numbers are not requested through either the FERPA or PPRA complaint form or through any other method by which information is collected. However, sometimes complainants or other parties to an enforcement action or technical assistance request may include them. In cases where SSNs are submitted, these numbers are redacted or deleted where appropriate.

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

☑ N/A

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

☑ N/A

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 system's fillable PDF forms, as approved by the Office of Management and Budget (OMB), include the following notices in section 4.2. This language is also included on the CMTS login page. Once SPPO launches the portal that will enable online submission

of FERPA and PPRA complaints, the privacy notice will also be added to the complaint submission page as well as the login screen where school officials and other complainants access the system.

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

Privacy Act Statement: The Department is authorized to solicit the information contained in this Form by 20 U.S.C. 1232g, h. Your disclosure of the information requested on this Form is voluntary, but if you fail to provide any of the information, it may result in, among other things, your complaint being dismissed or returned to you for additional clarification. The principal purpose for which the information requested on this Form will be used is to resolve your complaint and determine whether the educational agency or institution violated FERPA. The Department has published the routine uses for which the information requested on this Form may be used in a system of records notice entitled "Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA) Record Systems (18-05-02), which was last published in the Federal Register on June 4, 1999 (64 Fed. Reg. 30106, 30123-24). The routine uses include, but are not limited to, disclosing records to the educational agency or institution against which a complaint or self-initiated investigation has been made or the State Educational Agency in that State. The Department may modify and update this system of records notice, in which case that update in addition to the Department's other systems of records notices may be found at: https://www2.ed.gov/notices/ed-pia.html. The effects of not providing any of the requested information on this Form may include, among other things, that your complaint is dismissed or returned to you for additional clarification. Paperwork Burden Notice. According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid Office of Management and Budget (OMB) control number. The valid OMB control number for this information collection is 1880-0544. Public reporting burden for this collection of information is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering, and maintaining the data needed, and completing and reviewing the collection of information. Obligation to respond is voluntary. If you have questions on your individual submission of this form, write directly to: Student Privacy Policy Office, U.S. Department of Education, 400 Maryland Avenue, S.W., Washington, D.C. 20202-8520.

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?

Any and all information provided by complainants is done so voluntarily as individuals may provide as much information or as little as they are comfortable sharing throughout the course of SPPO's review of their complaint. In the event an individual would like to withdraw a complaint or technical assistance request and opt out of providing any more information, their ticket will be closed out and their information will be disposed of in accordance with the system's records retention schedule as indicated above.

Respondents are notified that failure to complete the complaint form in its entirety or failure to provide any of the information required for SPPO to determine whether a complaint contains specific allegations of fact giving reasonable cause to believe that a violation of FERPA or PPRA has occurred, may result in, among other things, the dismissal or return of the complaint in an effort to obtain additional information needed by SPPO to further consider the complaint. If the complaint is dismissed, the respondent may choose to submit a new complaint per the instructions set forth in the complaint form and in accordance with the requirements of FERPA or PPRA.

As part of the investigation, or self-initiated enforcement action as applicable SPPO will work collaboratively with education agencies to gather the information necessary to investigate the complaint. While a caseworker may request information pursuant to the investigation, a response from the education agency is voluntary. Education agencies who fail to respond to repeated requests for information will be informed that the investigation will proceed based solely on the input from the complainant.

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

Information gathered through the submission of a complaint, in response to a complaint or SPPO self-initiated enforcement action, data breach report, general technical assistance, or requests for policy clarification request may be shared with other offices in the Department, such as the Office of General Counsel (OGC)), Office of the Inspector General (OIG), Office of Special Education Programs (OSEP), Office for Civil Rights (OCR), and Federal Student Aid (FSA), on a case-by-case basis, if the assistance of the other office(s) is needed to conduct investigations or reach a determination regarding violations of FERPA or PPRA, or to respond to requests for technical assistance and other inquiries about these laws.

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

☐ N/A

To carry out its enforcement responsibilities under PPRA or FERPA and to provide technical assistance on student privacy, SPPO may share records with other offices in the Department for the purpose of obtaining assistance in processing or resolving a complaint or other enforcement action. SPPO may seek assistance from the OGC, which advises on legal matters related to FERPA and PPRA. For complaints and enforcement actions involving students with disabilities, SPPO may seek advice from OSEP. As needed, SPPO may also consult with or refer individuals to OCR pertaining to cases regarding civil rights or other matters within OCR's jurisdiction. Further, SPPO may also seek guidance from or refer individuals to FSA, as appropriate, when the case pertains to matters also impacting that office.

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

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

[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.

whom and for what purpose.

☐ N/A

SPPO does not share records in this system externally as part of its typical business processes; however, the office does have a need to share records externally in some instances. The Department may disclose information maintained in a record under the routine uses listed in the SORN without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. SPPO generally only discloses records outside of the Department in cases where the disclosure is necessary to effectively address the alleged violations of FERPA and PPRA, to resolve enforcement actions self-initiated by SPPO, or to maintain and respond to requests for technical assistance and other inquiries about these laws. Please see the SORN referenced in Question 2.2.1 for more details about permissible disclosures outside of the Department.

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

☐ N/A

SPPO generally does not share records externally; however, SPPO may share records externally in certain circumstances under the following routine uses:

(1) Member of Congress Disclosure. The Department may disclose records to a member of Congress from the record of an individual in response to an inquiry from the member made at the written request of that individual. The member's right to the information is no greater than the right of the individual who requested.

(2) Educational Agency or Institution. The Department may disclosure records from this system of records to an educational agency or institution against which a complaint has been made.

(3) State Educational Agency. The Department may disclose records to a State educational agency relative to an educational agency or institution in that State against which a complaint has been filed.

(4) Disclosure for Use by Other Law Enforcement Agencies. The Department may disclose information to any Federal, State, local or foreign agency or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation if that information is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility within the receiving entity's jurisdiction.

(5) Disclosure to the Department of Justice (DOJ). The Department may disclose records to the DOJ to the extent necessary for obtaining DOJ advice on any matter relevant to FERPA or PPRA investigations or other enforcement responsibilities under FERPA or PPRA.

(6) Contract Disclosure. If the Department contracts with an entity for the purposes of performing any function that requires disclosure of records in this system to employees of the contractor, the Department may disclose the records to those employees. Before entering into such a contract, the Department shall require the contractor to maintain Privacy Act safeguards as required under 5 U.S.C. 552a(m) with respect to the records in the system.

(7) Freedom of Information Act (FOIA) Advice Disclosure. The Department may disclose records to the Department of Justice and the Office of Management and Budget if the Department concludes that disclosure is desirable or necessary in determining whether particular records are required to be disclosed under the FOIA.

(8) Enforcement Disclosure. In the event that information in this system of records indicates, either on its face or in connection with other information, a violation or potential violation of any applicable statute, regulation, or order of a competent authority, the Department may disclose the relevant records to the appropriate agency, whether foreign, Federal, State, Tribal, or local, charged with the responsibility of investigating or prosecuting that violation or charged with enforcing or implementing the statute, executive order, rule, regulation, or order issued pursuant thereto.

(9) Litigation and Alternative Dispute Resolution (ADR) Disclosures.

(a) Introduction. In the event that one of the parties listed below is involved in litigation or ADR, or has an interest in litigation ADR, the Department may disclose certain records to the parties described in paragraphs (b), (c) and (d) of this routine use under the conditions specified in those paragraphs:

(i) The Department of Education, or any component of the Department; or

(ii) Any Department employee in his or her official capacity; or

(iii) Any Department employee in his or her individual capacity if the DOJ has agreed to provide or arrange for representation for the employee;

(iv) Any Department employee in his or her individual capacity where the agency has agreed to represent the employee; or

(v) The United States where the Department determines that the litigation is likely to affect the Department or any of its components.

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

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

☐ N/A

This information sharing would be done using either secure email exchange through the CMTS or using encrypted, password-protected content sent through the Department's standard email configuration.

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

No

6. Redress

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

If individuals wish to access the contents of their record(s) they may contact the system manager. The request must meet the requirements of the regulations at 34 CFR 5b.7. Please see the SORN referenced in Question 2.2.1 for more details.

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

If individuals wish to amend or contest the content of their record(s) they may contact the system manager. The request must meet the requirements of the regulations at 34 CFR 5b.7. Please see the SORN referenced in Question 2.2.1 for more details.

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

Instructions for accessing and amending records are provided in this PIA and in the SORN referenced in Question 2.2.1.

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 Authorization 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?

CMTS is hosted on the AWS Government cloud computing platform. Access to the system is limited to authorized Department users. The system limits data access to users on a "need to know" basis and controls individual users' ability to access and alter records within the system. Department employees are also required to complete security and privacy awareness training on an annual basis.

CMTS has a system of user access controls to ensure that users only have access to the information needed to fulfill their required tasks in the system. Each user, after their account is created in CMTS, is assigned to a particular "group" of accounts. These groups are customizable in terms of what access users have to other user information and what other information in CMTS they would be authorized to access. In the case of complainants, parties to enforcement actions self-initiated by SPPO, and data breach notifications, respondents are required to establish an account and are provided access only to their own user credentials and the information they submitted, as well as correspondence to which the Department has afforded them access. Since accounts are not required for technical assistance requests, requestors will not have access to

information submitted unless they request record access pursuant to the SORN. Requestors will be provided a response to their inquiry.

The CMTS Information System Owner (ISO) is responsible for daily operational oversight and management of the system's security and privacy controls and ensuring that the data are properly managed and that all access to the data has been granted in a secure and auditable manner. The CMTS ISO is responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the Department's Office of the Chief Information Officer, the SPPO, and the appropriate Department officials in accordance with Federal policy and established Department procedures.

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.

AWS CloudWatch and CloudTrail are used to monitor access to all data maintained on the CMTS. Logs are reviewed monthly and are indexed by AWS OpenSearch, which provides alerts of any anomalous behavior detected based on search patterns and known behaviors.

The system administrator runs required scans/tests on a monthly and annual basis as required. Security and system documentation are updated as required. Monitoring and auditing of all event logs are performed on a regular basis. Patches are checked for on a periodic basis and tested and applied to the server on a weekly basis, depending on necessity.

When going through the ATO/Ongoing Security Authorization (OSA) process, the system owner establishes monitoring processes to ensure the information is used in accordance with the approved practices. During the OSA process, smaller subsets of security controls are tested every quarter.

Following each patch release an additional scan is conducted to ensure continuing operations. Additional activities include conducting regular self-assessments, contingency plan testing, and participating in tabletop exercises.

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 that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, CMTS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner also ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in OSA, which addresses security and privacy risks throughout the system's life cycle.

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?

The CMTS includes potentially sensitive information about enforcement actions and technical assistance requests under FERPA and PPRA. This information could include allegations of violations and other information that describes sensitive facts about individuals. The nature of the information maintained in CMTS increases the privacy risks associated with a potential breach or improper disclosure, such as identity theft, embarrassment, or retaliation as a result of an investigation. Furthermore, additional PII may be obtained on a case-by-case basis via correspondence or the investigative process.

The inclusion of this additional, potentially sensitive information increases the privacy risks. In addition, similar to any organization, the Department is vulnerable to risks such as data breaches, phishing attempts, and server failure.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. 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.