Privacy Impact Assessment (PIA)
for the

Correspondence Tracking System (CTS)
September 2, 2022

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: Carla Reed/Senior Project Manager, Office of the Executive Secretariat
Contact Email: Carla.Reed@ed.gov

System Owner

Name/Title: Carla Reed/Senior Project Manager, Office of the Executive Secretariat
Principal Office: Office of Secretary (OS)

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 Correspondence Tracking System (CTS) is a system that tracks incoming and outgoing correspondence and other internal and external documents within the U.S. Department of Education (Department). CTS is a web application accessed through a browser that includes a SharePoint integration for storage of files.

CTS processes internal and external documents and correspondence. The kinds of external documents and correspondence that CTS processes include letters from the White House, Congress, and the public; requests for status of complaints; stakeholders' concerns about policy changes; and invitations. Internal documents tracked by CTS include decision, information, policy, and hiring memoranda; personnel actions[1]; Department enforcement actions; and books/gifts sent to the Secretary.

Department staff receive incoming correspondence, then manually enter information including writer's name and address, the date the correspondence was received, the subject, the priority level, and who should sign the outgoing correspondence. Documents may be received through either physical or electronic mail; physical correspondence is scanned to electronic files. The scanned or original emailed correspondence is then given a unique tracking number and stored in a SharePoint database. Staff use the system to track the status of the aforementioned documents, noting to whom they have been assigned for handling within the Department and when they have been completed. In addition, staff can also use the system to retrieve incoming and outgoing correspondence. Authentication for CTS users is done through the Identity, Credential, and Access Management (ICAM) system; usernames and passwords are not maintained in CTS.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected,

[1] Personnel actions include awards, retirements, separations, conversions, position changes, reassignments, details, pay changes, changes to position numbers, etc.
[2] 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

used, maintained or shared.

This system contains records about individuals who correspond with the Secretary, Deputy Secretary, Senior Officers, or other officials of the Department for whom the Department controls responses. The purpose for collecting PII in CTS is to account for the correspondence received by the Department. The information received is that which the sender chooses to include in the communication, but typically includes PII that is relevant for the topic/issue at hand.

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

CTS is replacing the Correspondence Control Manager (CCM) Plus system, therefore a new PIA is required.

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

Contractor

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

☐ N/A

Yes

2. Legal Authorities and Other Requirements

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

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

CTS is authorized by Title 5 – Government Organization and Employees, Section 301, Departmental regulations (5 U.S.C. 301).

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)).[3] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The Secretary's Communication Control System SORN, entitled the "Secretary's Communications Control System" (18-01-01), 83 FR 18544, was published in the Federal Register on April 27, 2018.

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.

The records disposition schedule is ED 062: Significant Correspondence.
Disposition: Permanent. Transfer nonelectronic records to the National Archives 10 years after cutoff. Transfer electronic records to the National Archives every 5 years, with any related documentation and external finding aids, as specified in 36 CFR 1228.270 or standards applicable at the time.

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

[3] 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 PII elements that are stored in the system are the sender's name, address, email address, and short summary of the communication. Correspondence received from the public and other sources may include other types of PII, including Social Security number (SSN), date of birth, place of birth, home address, home phone number, financial information, and medical information.

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

Yes

CTS collects only the minimum information necessary in order to respond to any correspondence from the public. Contact information, such as the individual's name, email address is used to communicate with the individual or entity. Individuals voluntarily provide information when they contact the Department.

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

PII is collected directly from the individuals/entities (e.g., school administrators, parents, students, advocacy groups, and any other member of the public) who send in the correspondence. PII is also collected from inquiries from the White House, or internal within the Department (e.g., Office of Legislation and Congressional Affairs).

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

Correspondences are received either by email or physical mail. If the correspondence is a physical letter, it is scanned and is placed in the system as a non-searchable PDF file. If the correspondence is an e-mail, it will also be saved as a non-searchable PDF file and stored in the system.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Individuals voluntarily provide information when they contact the Department. Validation relies on the individual providing correct contact information for the Department to respond to them.

Use

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

The information is used to track, manage, and account for the correspondence received by the Department, including individual concerns and complaints regarding programs administered by the Department. Additionally, reports of pending letters and reports on average response times are generated internally using this data so that the Office of the Secretary can ensure that responses are handled in a timely manner.

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

No

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

☑ N/A

Click here to enter text.

Social Security Numbers

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

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

[4] 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

If an individual or entity chooses to include an SSN in the communication, it will be retained on the scanned document. The SSN however, would not be entered into the database. The SSN would not be searchable as a separate data item, nor would the database indicate whether the SSN was included in the communication.

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.

Individuals or entities voluntarily provide information when they contact the Department. Notice of how their information is handled once submitted to the Department is provided through the publication of this PIA and the SORN referenced in 2.2.1.

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

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?

Individuals or entities voluntarily provide information when they contact the Department. They may decline to provide PII but choosing to do so will hinder the Department's ability to respond to their correspondence. Individuals or entities who submit any correspondence with the Department consent to how the information is tracked, managed, and accounted for within CTS in order to respond to the correspondence.

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

The PII shared with other Department principal offices[5] are name, address, email address and phone number (A phone number is typically not shared but if it is in correspondence document, then it is shared). The PII is shared with internal Department staff who have restricted access to CTS for their principal office's records. The PII is only shared with the intended principal office's staff that have job functions that require them to access correspondences.

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

☐ N/A

The purpose of sharing the PII with internal principal offices is so they can prepare or review responses to the correspondence. Reports are generated from the database in order to be used by the program office staff and their managers to view and track information about correspondences that have been assigned to their specific office. These reports typically include the name, email address, and phone number (if provided)

[5] There are 17 principal offices that utilize CTS for Correspondence and Document Clearance: Office of Secretary (OS), Office of the Under Secretary (OUS), White House Initiative on Historically Black Colleges and Universities (WHIHBCU), Federal Student Aid (FSA), Institute of Education Sciences (IES), Office of the Chief Information Officer (OCIO), Office of Communications and Outreach (OCO), Office for Civil Rights (OCR), Office of Career, Technical and Adult Education (OCTAE), Office of English Language Acquisition (OELA), Office of Finance and Operations (OFO), Office of the General Counsel (OGC), Office of Inspector General (OIG), Office of Legislation and Congressional Affairs (OLCA), Office of Postsecondary Education (OPE), Office of Planning, Evaluation, and Policy Development (OPEPD), and Office of Special Educational and Rehabilitative Services (OSERS).

of the sender and a summary of the purpose of the correspondence, as well as information such as date of letter, due date for response, and current status of the response.

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.[6]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

Generally, this information will not be disclosed to any other entity. If any correspondence is received from an entity acting on behalf of an individual, consent to share is validated prior to any information being shared with the third party. In addition, the Department may disclose information contained in a record in this system of records under the applicable routine uses without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected, i.e., tracking Department correspondence.

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

☐ N/A

See Question 5.5.

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

[6] 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.

The record of disclosure(s) is maintained within the correspondence record. The record details the individual or entity, the date in which a response was provided, and the data sent. A record of disclosure(s) can be made available upon request.

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

☐ N/A

Responses are provided typically through email. If an email is not provided, other methods (i.e., physical mail) are used to provide a response to the correspondence.

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 an individual wishes to access the content of a record in this system of records, he or she should contact the system manager with necessary particulars such as name, the date of the subject documents, a reasonable description of the subject matter of the issue involved, and any other identifying information requested by the Department while processing the request needed to distinguish between individuals with the same name. The individual must meet the requirements in 34 CFR 5b.5, including proof of identity.

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

If an individual wishes to contest the content of a record in this system of records, he or she should contact the system manager and reasonably identify the record and specify the information to be contested. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

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

Individuals or entities are notified about the procedures for correcting their information on the published SORN.

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?

CTS resides in the Department network and follows Department risk assessment policy and procedures. The following guidelines and procedures have been implemented for protecting system sensitive data and resources. The system has role-based access governed by the need-to-know principle; user must have a necessary need to access the system for their job functions. Access to the system is limited to a small number of users (approx. 150 users Department-wide) who manage correspondence inquiries for their program office. The system owner performs a quarterly review of user accounts to ensure the accounts are needed and accurate. The system is PIV-enabled which also ensures users are active and credentialed Department employees. Therefore, Department employees who separate from service cannot access the system because their PIV card has been revoked, ensuring another layer of protection.

All physical access to the system on site is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge. During working hours, direct access to the file cabinets is limited to authorized staff. During non-working hours, the rooms in which the file cabinets are located are locked and only those individuals with access to those rooms can access the hard copies of records.

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.

The following tasks are performed to safeguard CTS information:

- Monthly vulnerability scans performed.
- Annual contingency plan test performed.
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team.
- Annual updates to system security documents.
- Annual mandatory cybersecurity and privacy training for employees and contractors.
- Employees and contractors who are provided access to the system have to sign a Rules of Behavior.

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 stated practices in this PIA. A portion of the security controls are assessed quarterly to ensure an annual assessment of all controls for the system to maintain its ATO. Users who access data in this system must comply with the requirements of the Privacy Act

and the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573), which provides criminal penalties for violations. Access to information is strictly controlled. Staff with access to the system are required to complete annual security and privacy awareness training. In addition, they are required to have background clearance at the 5c level or higher.

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?

Privacy risks associated with CTS are low because the system in internal facing and data is encrypted while in use, in transit and at rest. 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, 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 per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.