



Privacy Impact Assessment (PIA)
for the

Control Correspondence Manager Plus

February 6, 2020

For PIA Certification Updates Only: This PIA was reviewed on **February 6, 2020** by **Stephanie Williams** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Stephanie Williams
Contact Email: Stephanie.Williams@ed.gov

System Owner

Name/Title: Stephanie Williams, Acting Deputy Director, 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 Department of Education utilizes the Secretary's Communications Control System (also known as CCMEnterprise and CCMPlus) to track official correspondence of the Secretary, Deputy Secretary, Senior Officers, or other officials of the Department for whom the Department controls responses, including correspondence regarding individual concerns and complaints regarding programs administered by the Secretary.

There are currently 17 Principal offices that utilize CCM Plus for Correspondence:

1. Office of Secretary (OS)
2. Office of the Under Secretary (OUS)
3. White House Initiative on Historically Black Colleges and Universities (WHIHBCU)
4. Federal Student Aid (FSA)
5. Institute of Education Sciences (IES)
6. Office of the Chief Information Officer (OCIO)
7. Office of Communications and Outreach (OCO)
8. Office for Civil Rights (OCR)
9. Office of Career, Technical and Adult Education (OCTAE)
10. Office of English Language Acquisition (OELA)
11. Office of Finance and Operations (OFO)
12. Office of the General Counsel (OGC)
13. Office of Inspector General (OIG)
14. Office of Legislation and Congressional Affairs (OLCA)
15. Office of Postsecondary Education (OPE)
16. Office of Planning, Evaluation, and Policy Development (OPEPD)
17. Office of Special Educational and Rehabilitative Services (OSERS)

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

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](#)

The purpose for collecting PII in CCM Plus is to account for the correspondence received by the Department. The information received is that which the sender chooses to include in the communication.

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

Currently Operating System

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

Updated PIA

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

Agency

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

N/A

[Click here to select.](#)

2. Legal Authorities and Other Requirements

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

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

The authorizing statute is TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES U.S.C. 301 Departmental regulations.

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

Secretary's Communications Control System (18-01-01) 83 FR 18544, dated April 27, 2018. <https://www.federalregister.gov/documents/2018/04/27/2018-08962/privacy-act-of-1974-system-of-records>.

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

2.3. 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.

The records schedule number is N1-441-08-19.

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

Yes

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>

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 senders name, address, email, and short summary of the communication. The communication may also include additional personal information depending on the nature of the correspondence.

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

Yes

- 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 who send in the correspondence.

- 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 paper mail or email. If the correspondence is a paper 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?³ 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.

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.

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

Social Security Numbers

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

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

No

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

N/A

If an individual chooses to include an SSN in the communication, it will be retained on the scanned document. 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

[Click here to enter text.](#)

4. Notice

- 4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Individuals 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

[Click here to enter text.](#)

- 4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Individuals 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.

- 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 is name, address, email and phone number (A phone number is typically not shared but if it is in correspondence document, then it is shared). The PII is based on what was provided by the individual who wrote in. The PII is shared with internal ED staff who have restricted access to CCM for their Principle Office's records. The PII is only shared with the intended Principle 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 Principle Offices is so they can prepare or review responses to the correspondence. The reports that are generated from the database are 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 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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.⁴

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

N/A

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

N/A

⁴ If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

N/A

[Click here to select.](#)

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

N/A

[Click here to select.](#)

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

N/A

[Click here to enter text.](#)

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

N/A

[Click here to select.](#)

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

N/A

[Click here to select.](#)

6. Redress

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

If you wish to determine whether a record exists regarding you in this system of records, contact the system owner listed on the SORN Secretary's Communication Control System (18-01-01). You must provide necessary particulars such as your 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.

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

Individuals can contact the original sender via correspondence (via physical mail or email) to correct any incorrect information. Individuals may also contact the system owner listed on the SORN to correct any inaccurate or erroneous information.

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

Individuals are notified about the procedures for correcting their information on the published SORN. Additionally, individuals are also notified by mailed letter or email.

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?

The Secretary's Communications Control System 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

ED employees. Therefore, ED 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.

The computer systems employed offer a high degree of resistance to tampering and circumvention.

- 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.

Weekly vulnerability scans are conducted and reviewed at the server level.

Sensitive data, such as that covered by the Privacy Act, is protected from unauthorized disclosure, modification, and destruction. Security audits are performed on annual basis by authorized third parties to ensure the controls in place are effectively securing the data.

The system recently went through a new ATO and was approved. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones (PO&AMs) to remediate any identified deficiencies, and a continuous monitoring program.

Users are required to complete the Department's mandatory Cybersecurity and Privacy Awareness courses and accept the rules of behavior in order to gain access to departmental network which is used to access the system.

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 by working closely with the Privacy Office to make sure all privacy related documents are updated and current. The system owner also participates in all major security and privacy risk briefings. Further, with the use of the following provisions, the system owner ensures privacy is sufficiently protected: (1) Limited number of user accounts and accounts are only provided to Department employees who work specifically on correspondence; (2) Users can only access the system using Department of ED PIV card ; (3) System workflows are designed using “Need to Know” philosophy.

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 privacy risk associated with this system is unauthorized access. The privacy risk is mitigated by limiting access to the system to only those who work specifically on correspondences. The system also can only be accessed using a Department of ED PIV card, prevent unauthorized access. The system also includes a firewall to protect, detect, monitor, alert, or block attacks onto the system. The system owner routinely reviews that access levels are adequate for each user accessing the system.