Privacy Impact Assessment

For the Secretary’s Communications Control System

Date: March 21, 2016

Point of Contact:
Deborah Winters
Deborah.Winters@ed.gov

System Owner:
Director, Office of the Executive Secretariat

Author:
Deborah Winters
Deborah.Winters@ed.gov

Office of the Secretary

U.S. Department of Education
1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

   The Department of Education utilizes the Secretary’s Communications Control System to track official correspondence between 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.

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

   The authorizing statute is 5 U.S.C. 301.

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

   The information received is that which the sender chooses to include in the communication. Only the sender’s name and address and/or email address, and a short summary of the communication, are logged into the Communications Control System. If the communication is a paper letter, it is scanned and is placed in the record, usually as a non-searchable PDF file. If the communication is an e-mail, it can be saved to the record, usually in MSG or TXT format, or it can be printed out and scanned in like a paper letter.

4. **Why is the information collected?** How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

   This information is collected when individuals communicate with the Office of the Secretary, the Deputy Secretary, Senior Officers or other officials of the Department for whom the Department controls responses. The information is provided voluntarily by the communicant, and is collected and maintained in the system so that correspondence to the Department can be assigned internally for response, tracked to ensure that an appropriate response is generated in a timely manner, and retrieved as needed to fulfill requests such as FOIA requests.

5. **Social Security Number (SSN).** If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.
If an individual 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.

6. **Uses of the Information.** What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

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.

7. **Internal Sharing and Disclosure.** With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

Access to records is limited to those ED users with a business need to access the record, such as those assigned to prepare or review responses to correspondence. In addition, reports are generated from the database to provide Program Office staff and their managers with information about correspondence that has 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.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

Generally, this information will not be disclosed to any other entity. However, the Department of Education 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. Possible disclosures include:

- Government and Private Organization Disclosure
- Congressional Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosures
- Disclosure to Recipients of Federal Financial Assistance, Witnesses, or Consultants
Privacy Impact Assessment

- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Freedom of Information Act (FOIA) Disclosure
- Research Disclosure
- These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act, under a computer matching agreement.

Additionally, the Department may disclose to a consumer reporting agency information regarding a claim by the Department which is determined to be valid and overdue as follows: (1) The name, address, taxpayer identification number and other information necessary to establish the identity of the individual responsible for the claim; (2) The amount, status and history of the claim; and (3) The program under which the claim arose.

9. Notice. Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Not applicable. Individuals voluntarily provide information when they contact the Department.

10. Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.

Not applicable.

11. Security. What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?


Sensitive data, such as that covered by the Privacy Act, needs to be protected from unauthorized disclosure, modification, and destruction. The following guidelines and procedures have been implemented for protecting System sensitive data and resources.
• All physical access to the Department of Education sites are controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

• Direct access to the file cabinets is limited to authorized staff.

• 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 by the Department of Education offer a high degree of resistance to tampering and circumvention.

12. Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

The authority for the Department to maintain these records is an existing system of records (SORN) entitled Secretary’s Communications Control System (18-01-01).

13. Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

The records disposition schedule is ED 062: Significant Correspondence Files. Disposition: Permanent. Hard copy records are transferred to the Washington National Records Center one year after cutoff then transferred to the National Archives and Records Administration (NARA) 10 years after cutoff. Control records on computer are stored indefinitely. Electronic images are retained based on regular records disposal or retention policies identical to hard copies.

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