Privacy Impact Assessment (PIA)
for the

Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA

Nov 12, 2018

This PIA was originally approved on Nov 6, 2018 and reviewed on Nov 6, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Frank Miller/Deputy Director/ Family Policy Compliance Office

Contact Email: Frank.E.Miller@ed.gov

System Owner

Name/Title: Chief Privacy Officer

Program Office: Office of Management (OM)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.***

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

The Department of Education's Office of the Chief Privacy Officer (OCPO), through the Family Policy Compliance Office (FPCO), utilizes this system to receive, review, and attempt to resolve disputes regarding violations of FERPA and PPRA. The system operates as a case tracking system to track, monitor, and close out tickets associated with each individual dispute.

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

Information contained in this system is used to resolve complaints alleging violations of FERPA and PPRA. While a copy is maintained in this system, requests for technical assistance are forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance.

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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

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? If this is an update, please include the publication date of the original.

New PIA Original Publication Date:

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

Agency

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?

Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 CFR part 99) and 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? Please answer **YES** or **NO**.

Yes

2.2.1 ☐ N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name and number, or indicate that a SORN is in progress.

Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendments (PPRA) Record System (18-05-02) published in the Federal Register on June 4, 1999 at 64 FR 30123.

https://www2.ed.gov/notices/sorn/18-05-02_060499.pdf

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 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Inquiry records are maintained a minimum of three years; complaint and investigative records are maintained a minimum of six years after the case is closed. Inquiry records are maintained in accordance with Department of Education Records Disposition Schedule ED 162: Family Policy Compliance Office Complaints and Technical Assistance. The NARA Disposition Authority number is N1-441-09-18.

[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

2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

This system consists of complaints alleging violations of FERPA or PPRA and correspondence making requests for technical assistance or other inquiries about these laws. General information pertaining to complaints and correspondence may include first and last names, addresses, phone numbers, dates of birth, and email addresses. Additional personally identifiable information may be obtained on a case-by-case basis via correspondence or 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 the educational institution. Please note that while we do not request Social Security numbers, there are times when the complainant includes them when submitting supplemental information.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

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

This system covers information that is collected directly from the parent or eligible student who maintains FERPA rights over the education records that are the subject of the complaint, or an attorney or advocate filing on his or her behalf. We may also receive information from schools, districts and colleges/universities as requested during the investigation process.

3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

Complaints and correspondence are submitted in paper form, electronically via email or through the student privacy website at https://studentprivacy.ed.gov/. While a copy is maintained in this system, requests for technical assistance are forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance.

3.5 How is this information validated or confirmed?[3]

As stated above, the information is gathered directly from the complainant or an attorney/advocate on their behalf, through an Information Collection/OMB approved form. Upon receipt, the Department sends an acknowledgment letter or email to the individual. These forms are then reviewed for completeness and clarity, with any concerns verified by the complainant either through phone call or written request. While a copy is maintained in this system, requests for technical assistance are forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance.

[3] Examples include form filling, account verification, etc.

Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

Information contained in this system is used to first determine if the complaint is filed by an individual who maintains FERPA 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 has occurred. If those conditions are met, the information in the system is then used to resolve disputes regarding violations of FERPA and PPRA. While a copy is maintained in this system, requests for technical assistance are forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

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

3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 ☒ N/A If the above answer is **YES,** please explain.

Social Security Numbers

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

3.9 Does the system collect Social Security Numbers? Please answer **YES** or **NO**.

No

3.9.1 ☐ N/A If the above answer is **YES,** explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

We do not request social security numbers on our complaint forms. However, there are rare occasions where there individual will include SSN's when submitting supplemental information. Although not requested or required, the SSN will be sufficiently safeguarded.

3.10 ☒ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

Under this system, individuals either receive the Privacy Act notice as embedded content in the complaint form itself, or via a link to the Department's Privacy Act notice. Both of which are included below.

4.2 ☐ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

Privacy Act Statement. The Department is authorized to solicit the information contained in this Form by 20 U.S.C. 1232g(f) and (g) and 34 CFR part 99, subpart E. 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, 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 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 result in your complaint being dismissed or returned to you for additional clarification. In addition, here is a link form our student privacy website: https://studentprivacy.ed.gov/

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All information provided is voluntary and individuals may provide as little or as much information as they are comfortable with throughout the course of FPCO's review of their case. In the event an individual would like to cancel a claim 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 systems records retention schedule as indicated below.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2 ☐ N/A What information will be shared and with whom?

The complaint and correspondence information gathered, including requests for technical assistance, is shared without consent to other Offices in the Department, e.g. OGC, OSEP, FSA on a case-by-case basis if the assistance of the other Offices is imperative to resolve disputes regarding violations of FERPA and PPRA and to maintain and respond to requests for technical assistance and other inquiries about these laws. Any disclosure of FERPA-protected personally identifiable information obtained by the Department from students' education records would also have to be permissible under FERPA in terms of each of the routine uses listed in the SORN referenced in Section 2.2.

5.3 ☐ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

To carry out its enforcement responsibilities under the PPRA or FERPA, FPCO may share records with other offices in the Department for the purpose of obtaining assistance in processing a claim or resolving a dispute. FPCO may seek assistance from the attorneys who advise on FERPA and PPRA and reside in the Office of the General Counsel. For claims involving students with disabilities FPCO may seek advice from the Office of Special Education Programs. As needed, FPCO may also consult with, or direct individuals to the Office for Civil Rights pertaining to cases regarding discrimination or potential Title IX concerns. Further, FPCO may also seek guidance from, or again refer individuals to, Federal Student Aid (FSA) as appropriate when the case pertains to matters also impacting that office.

In addition, while a copy is maintained in this system, requests for technical assistance are forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance.

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

Yes

5.5 ☐ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

FPCO does not intend to share records in this system externally however it is permissible in some instances. The Department may disclose information contained in a record under the routine uses listed in the System of Records Notice (SORN) without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected and if the disclosure is critical to resolve disputes regarding violations of FERPA and PPRA and to maintain and respond to requests for technical assistance and other inquiries about these laws. Please see the SORN referenced in Section 2.2 for more details.

5.6 ☐ N/A What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

FPCO does not intend to share records externally however in the event that it is permissible under a routine use listed in the System of Records Notice, the disclosure will be compatible with the purposes for which the record was collected and critical to resolving disputes regarding violations of FERPA and PPRA and to maintain and respond to requests for technical assistance and other inquiries about these laws, including those referred to CPO's Student Privacy Policy and Assistance Division (SPPAD) for processing. Please see the SORN referenced in Section 2.2 for more details.

5.7 ☐ N/A How is the information shared and used by the external entity?

Please see the SORN referenced in Section 2.2 for more details.

5.8 ☐ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

No

5.9 ☐ N/A Does the project place limitation on re-disclosure? Please answer **YES** or **NO**.

Yes

6. Redress[4]

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

If individuals wish to access the content of a record regarding you in the system of records, they may contact the system manager. Your request must meet the requirements of the regulations at 34 CFR 5b.7. Please see the SORN referenced in Section 2.2 for more details.

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

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

If individuals wish to contest the content of a record regarding you in the system of records, they may contact the system manager. Your request must meet the requirements of the regulations at 34 CFR 5b.7. Please see the SORN referenced in Section 2.2 for more details.

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

Please see the SORN referenced in Section 2.2 for more details.

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? Please answer **YES** or **NO**.

Yes

7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

The information gathered through complaints and correspondence, as well as requests for technical assistance, are maintained in electronic files. Specifically, the complaints and correspondences, are maintained in modified version of the Department's Controlled Correspondence Management System (CCM). In addition, a copy of the requests for technical received by FPCO are also maintained in CCM, although forwarded to OCPO's Student Privacy Policy and Assistance Division (SPPAD) who is responsible for the provision of that assistance. Electronic files are only accessible by Department employees and contractors granted permissions though the Department's network administration. The Department also utilizes a hard copy backup to the electronic filing. These hard copy records are maintained in lockable file cabinets only accessible by designated staff.

7.3 What administrative, technical, and physical safeguards are in place to protect the information?

All physical access to the sites where this system of records is maintained and controlled is monitored by security personnel who check each individual entering the building for his or her employee badge. Paper files are kept in locked file cabinets when not in use. Immediate access to these records is restricted to authorized staff. Authorized staff members and contractors have unique user names and passwords that must be used to gain access to the electronic files. A system-access protocol requires the use of a passwords meeting minimum character and length specifications, and that these passwords be changed on a regular basis.

7.4 Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

Yes

7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

The Department conducts a variety of security testing activities across the enterprise as part of an overall risk management and continuous monitoring strategy. Some of these activities are ongoing, including infrastructure scans and Ongoing Security Authorization assessment testing, and some are performed as needed for major system changes, including ad hoc scans, Production Readiness Reviews, Security Impact Analyses, and system self-assessments.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

All Department staff and contractors with access to the information maintained as part of this system, receive initial training as part of the orientation process. In addition, staff and contractors must complete annual training on topics such as cyber-security and records management.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

While basic contact information is often times considered to have a lower risk to privacy, the individuals who's information is maintained in this system are collectively identified as individuals who's rights guaranteed under FERPA or PPRA have potentially been violated. This increases the privacy risk. Furthermore, on a case-by-case basis additional personally identifiable information may be obtained via correspondence or the investigative process. The inclusion of this additional, potentially sensitive, information increases the privacy risks. However, the Department, as with any organization with electronic records, is vulnerable to risks such as data breaches, phishing attempts, server failure, etc. No organization can be 100% protected, but by implementing a proactive data security plan, the Department can mitigate those risks.