Privacy Impact Assessment (PIA)
for the

OCR Complaint Assessment System
December 11, 2020

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: Jacqueline C. Lumford/Information Technology Specialist
Contact Email: Jacqueline.Lumford@ed.gov

System Owner

Name/Title: Jacqueline C. Lumford/Information Technology Specialist
Principal Office: Office for Civil Rights

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 Office for Civil Rights (OCR) Complaint Assessment System (OCRCAS) allows potential complainants to submit civil rights complaint information to the U.S. Department of Education (Department). The system contains: a pre-assessment to determine if a complaint can be considered, an online complaint form, and a backend database.

Pre-Assessment

The pre-assessment is an optional real-time tool that allows a complainant to answer six multiple choice questions to assist in understanding if a complaint meets the OCR standards of a complaint. At the end of the assessment, depending upon how questions are answered, the complainant will either get a message stating they can move forward with the complaint or resources at other federal, state, or local government to reach out to for further assistance if the answers provided do not rise to the level of a formal complaint. In either scenario, if the complainant wishes to submit a complaint, there is a link to the complaint form (described below). Answers provided to the pre-assessment are not collected or maintained by OCRCAS.

Complaint Form

If the complainant decides to move forward with a complaint, there are multiple ways in which a complaint can be filed: 1) OCR online complaint form, or 2) downloading a PDF of the complaint form and either emailing, mailing, or faxing the completed form.

- **Online Complaint Form**
  For a submission through the online complaint form, the description of the proposed complaint is submitted by the requester on the form. Once submitted , the complaint is sent to a middleware database maintained within the Case and Activity Management System (CAMS) boundary so that regional offices can access the complaint for processing. Regional offices evaluate specific details of a complaint and determine if a complaint warrants further investigation. If an investigation is required, the regional office will assign a document number to the complaint and submit it formally

into CAMS. Complaint submissions are given an OCR Electronic Complaint Submission ID.

- **Physical Complaint Form**
  If a complainant decides to send the complaint form through email, mail, or fax, the information contained within the physical form is then manually entered into OCRCAS by OCR staff and follows the process as identified in the paragraph above.

OCRCAS enables the public to submit their initial complaint to the Department. The OCRCAS backend database maintains all collected data for a six-month period and then is deleted.

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

The system allows for potential complainants to submit civil rights complaint information to Department. The information is used to contact the requester and perform an initial analysis to determine if the submission is indeed a complaint that the Department will need to pursue, and to route the complaint to a regional office for further investigation.

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 – An update to the PIA was required to accurately represent the PII collected by the system.

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 information is collected under the authority of the six Federal civil rights statutes that OCR enforces:

- Title VI of the Civil Rights Act of 1964, prohibiting discrimination on the basis of race,color, and national origin;
- Title IX of the Education Amendments of 1972, prohibiting discrimination on the basisof sex;
- Section 504 of the Rehabilitation Act of 1973, prohibiting discrimination on the basis of disability;
- Title II of the Americans with Disabilities Act of 1990, prohibiting discrimination on thebasis of disability;
- Age Discrimination Act of 1975, prohibiting discrimination on the basis of age; and
- Boy Scouts of America Equal Access Act of 2001, prohibiting the denial of equal access or a fair opportunity to meet to the Boy Scouts of America or other listed youth groups.

These civil rights laws enforced by OCR extend to institutions that receive Federal financial assistance from the Department and institutions for which OCR has been delegated authority from other Federal agencies, including state education agencies, elementary and secondary school systems, colleges and universities, vocational schools, proprietary schools, state vocational rehabilitation agencies, and libraries.

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

Information is retrieved by an identification (ID) number assigned to the individual who submitted the complaint.

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)).[1] Please provide the SORN name, number,

[1] 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

Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Complaint Files and Log (18-08-01), Document Citation (83 FR 12571)

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.

ED 026: Education Discrimination Case Files (N1-441-08-6). Disposition: Temporary. Cut off at the end of the fiscal year in which the case is closed and monitoring is completed, or, if a Request for Reconsideration (RFR) is received, when the review of the RFR is completed. Destroy/delete 20 years after cutoff. For significant case files disposition is permanent. Cut off at the end of the fiscal year in which the case is closed and monitoring is complete. Transfer nonelectronic records to the National Archives every 5 years, with any related documentation and external finding aids, as specified in 36 CFR 1228.70 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?

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.

For complainants: First name, last name, address, primary phone number, alternate phone number, email address, alternate contact name (if individual providing complaint cannot be reached), alternate contact phone number, institution name (of institution that allegedly discriminated against the complainant), institution address, and basis of perceived discrimination (check boxes: race or color, national origin, disability, sex, age, retaliation because you filed a complaint or asserted your rights, Boy Scouts Equal Access Act). In addition, there are two optional free-form text boxes that allow for:

- Additional description for the alleged discrimination.
- Any remedies the complainant is requesting.

For system administrators: Name, email address, username, password.

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

Yes

The PII elements listed in Question 3.1 are the minimum information that OCR needs for the initial processing of the complaint and for potential routing to a regional office for further investigation.

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

The information is provided by members of the public who submit a civil rights complaint to the Department.

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 complainant submits the information using the electronic discrimination complaint form. If a complainant does not have access to the electronic discrimination complaint form, a fillable PDF form can be completed and submitted through email, mail, or fax.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[2] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

[2] 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 complainant submits information directly into the system through the website or through a fillable PDF form that is then emailed, faxed, or mailed to the Department. The information is used to contact the complainant to perform an initial analysis. If the complainant is not contacted because the information is incorrect, the complainant has the option to contact the Department again to inquire about the status of their complaint and fix the error in the information that was provided. The information regarding the basis for the civil rights complaint will be verified by OCR investigators if a complaint is routed to a regional office for further investigation.

Use

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

The information is used to contact the complainant and perform an initial analysis to determine if the submission is indeed a complaint that the Department will need to pursue, and to route the complaint to a regional office for further investigation.

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.

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

Click here to enter text.

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.

A Privacy Act statement found on the on the OCR complaint form website provides notice to the public. Additionally, this PIA and the SORN, Complaint Files and Log (18-08-01), also provide notice.

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

https://www2.ed.gov/about/offices/list/ocr/edlite-notice.html

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?

There is a "OCR Complaint Consent Form" on the complaint form website that allows individuals to consent to the use of their information. Prior to the completion of the initial processing of a complaint, complainants are required to provide the signed consent form authorizing the Department to proceed with the complaint.

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.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.[3]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

[3] 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.

☑ 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

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?

This system is exempted from the provisions of the Privacy Act that allow for access. See 34 CFR 5b.11(c)(2)(iii).

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

This system is exempted from the provisions of the Privacy Act that allow for the individual to request amendment. See 34 CFR 5b.11(c)(2)(iii).

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

This system is exempted from the provisions of the Privacy Act that requires notification regarding access and amendment. See 34 CFR 5b.11(c)(2)(iii).

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 system is maintained on secure computer servers located in one or more secure Department network server facilities. The system is only accessible and available to authorized Department and contract employees utilizing various authentication mechanisms including usernames and passwords. The system also limitsdata access by type of user and controls users' ability to alter records within the system.Records containing PII in the database are encrypted when at rest and in transmission.

Access to OCR offices is controlled and available only to OCR staff and authorized visitors. Access to the building is monitored by security personnel who check everyone entering the building for his or her employee or visitor badge. All Department and contract personnel who have facility access and system access are required to undergo a security clearance investigation. Department and contract employees are also required to complete security and privacy awareness training on an annual basis.

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.

OCRCAS participates in the Department's risk management framework processes in order to receive an authorization to operate (ATO). During this process, the security and privacy controls are checked for appropriate implementation and documentation.

The system is tested after every IT software patch to ensure the implemented patch did not adversely affect any of the security controls. Also, the ISSO performs challenge tests using invalid usernames and passwords annually and ISSO conducts user validation quarterly and during staff separation process.

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 approves or is given direction by senior leadership to authorize specific staff access to the application. These staff are required to undergo the Department's Privacy Act, Freedom of Information Act, Security, and additional trainings.

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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

One privacy risk associated with this system is unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud.

The risks are mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.

Another privacy risk could entail human error related to database management. This risk is managed through the application of several controls identified in the system security plan (access controls, configuration management, audit and accounting, identification and authorization, boundary controls, etc.).

Additional privacy risks for requesters and third parties are mitigated as OCR retrieves their cases by assigned ID number, not requester name. Further, as noted above, OCRCAS can be accessed only by employees and OCRCAS contractors, who have been subject to security clearances and are required to undergo regular trainings, including on the subject of protecting PII, and whose access to the system is tracked by the system. In addition to this, OCR employees are trained on how to protect PII.