Privacy Impact Assessment (PIA)
for the
Case and Activity Management System (CAMS)
June 26, 2017

Contact Point
Ting-Ting Wang / Information Technology Specialist
(202) 453-5944

System Owner
Ting-Ting Wang / Information Technology Specialist

Author
Ting-Ting Wang

Office for Civil Rights

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education
Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.

Please complete this Privacy Impact Assessment (PIA) on how information in identifiable form 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.

Introduction

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

The Office for Civil Rights (OCR) utilizes the Case and Activity Management System (CAMS) that contains two in-house developed applications, the Case Management System (CMS) and the Activity Management System (AMS), and one commercial-off-the-shelf (COTS) software, Open Text eDOCS Document/Record Management System (eDOCS DM/RM).

The CAMS supports OCR’s mandate to enforce six Federal statutes that prohibit discrimination by recipients of Federal financial assistance. OCR uses CAMS to manage record-keeping on the investigation of complaints, proactive investigations, and other civil rights activities more effectively and efficiently. CAMS tracks both case processing and other activities carried out by the OCR field and headquarters offices. CAMS also stores, maintains, and disposes of electronic and physical documents and records in keeping with applicable record-retention laws.

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

In the course of investigating a complaint, OCR staff collects the complainant’s name, address, and telephone number; the specific allegations of discrimination at issue; and other facts gathered in investigation of the allegations. OCR staff then input this information into CAMS to assist with record-keeping of investigations.

CAMS resides in the Department’s network and access is restricted to only OCR employees and CAMS contractors. Any contractor responsible for the operations of the

---

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.

CAMS is held to the privacy and security requirements of the Department in the handling of information collected through the system.

PII that is collected by staff and stored in CAMS may be shared in the course of an investigation. For example, if a student alleges that his or her school has discriminated against him or her, OCR may have to share some PII with the school in order to investigate the complaint. As specified on its website, OCR obtains the written consent of a complainant before sharing PII.2

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

The CAMS is currently in operation.

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

This PIA is an update of a previous version. The original one was published on August 10, 2007.

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

The CAMS is operated by the 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?

OCR enforces six Federal civil rights statutes. Discrimination on the basis of race, color, and national origin is prohibited by Title VI of the Civil Rights Act of 1964; sex discrimination is prohibited by Title IX of the Education Amendments of 1972; discrimination on the basis of disability is prohibited by Section 504 of the Rehabilitation Act of 1973; and age discrimination is prohibited by the Age Discrimination Act of 1975. These civil rights laws enforced by OCR extend to all state education agencies, elementary and secondary school systems, colleges and universities, vocational schools, proprietary schools, state vocational rehabilitation agencies, libraries, and museums that receive U.S. Department of Education funds.

2 https://www2.ed.gov/about/offices/list/ocr/complaintintro.html.
Enforcement of these statutes includes OCR having to investigate complaints filed by members of the public who allege they have been discriminated against. In order for people to file complaints of discrimination with OCR, and for OCR to investigate those claims, OCR must collect PII and that PII is then stored in CAMS.

Users are provided notice of rights under the Privacy Act via links to the agency Privacy Act regulations (34 C.R.F. Part 5b) and to the Privacy Act System of Records notice for the Complaint Files and Log, Number 18-08-01 (69 Fed. Reg. 12248) March 15, 2004.

**SORN**

2.2. Is the information in this system retrieved by name or personal identifier? If so this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s))? If no, explain why not. If yes, provide the SORN name and number, or indicate that a SORN is in progress.

The information in CAMS can be retrieved by name. CAMS is covered by a Privacy Act System of Records Notice (SORN). The SORN # is 18-08-01, Complaint Files and Log.

**Records Management**

*If you do not know your records schedule, please consult with your records liaison or RMHelp@ed.gov.*

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

A records retention schedule for CAMS has been approved by the National Archives and Records Administration (NARA). The NARA schedule numbers for this are ED 026 (a).1. ED 026 (a).2. ED 026 (b), ED 026 (c), ED 026 (d).

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
OCR added a record disposal function in FY2017 and plans in FY2018 to deploy this function, if budget permits.

Currently, the paper files are the official copies for applying the records disposition schedule. OCR is in the process of appropriate disposal in accordance with the timelines in the records disposition schedule.

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.

1) Names, addresses, and telephone numbers of complainants, complaint allegations, and, if applicable, the age, race and sex of alleged victims and other results of investigations;
2) Correspondence related to the complaint, which may include copies of correspondence sent by OCR to others, correspondence received by OCR, records of telephone conversations, copies of e-mail, or other written communications;
3) Investigator and attorney memoranda;
4) Interview notes or transcriptions and witness statements;
5) Documents gathered during an investigation, including photographs of persons or things, portions of a recipient institution’s records, and complainants’ or other individuals’ scholastic, medical, or employment records; and
6) Charts, prepared exhibits, or other analytical materials prepared by OCR staff or by consultants retained by OCR.

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

OCR staff does not seek information that is not required to resolve a complaint. Staff input the information obtained during an investigation into CAMS.

3.3. What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.), how is the information collected from stated sources (paper form, webpage, database, etc.), and how is this information validated or confirmed?4

---

4 Examples include form filling, account verification, etc.
Information is collected from individuals, K-12 schools, postsecondary institutions and other entities as applicable.

The information is collected from stated sources via oral interviews, paper form, webpages and electronic files.

The information is validated or confirmed by the staff assigned to the case.

Use

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

CAMS supports effective implementation of OCR’s mandate to enforce six Federal statutes that prohibit discrimination by recipients of Federal financial assistance. OCR uses CAMS to manage complaints, compliance reviews, and other civil rights activities more effectively and efficiently. CAMS tracks both case processing and other activities carried out by the OCR field and headquarters offices. CAMS stores, maintains, and integrates documents to permit end-to-end electronic processing of cases and activities. The benefits to OCR are electronic access to, retention, and integration of, documents and processes critical to fulfilling OCR's law enforcement mission.

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 the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.5. Does the system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures. *Please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.*

OCR’s Complaint Form does not ask for an individual’s Social Security Number. However, at times Social Security Numbers are contained in other records that are collected by OCR, such as medical records. OCR will have an internal procedure to ensure not including SSN while uploading written materials to CAMS.

3.6. Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

OCR’s Complaint Form does not ask for Social Security Numbers.
3.7. 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.

OCR provides information of its Investigatory Use of Personal Information on its Complaint Form (pages #11-12). OCR also informs complainants that a signed, written consent form may be required in order for OCR to proceed with an investigation.

There is also a published Privacy Act Notice, SORN #18-08-01, Complaint Files and Log.

3.8. Provide the text of the notice, or the link to the webpage where notice is posted.

Information about consent form:
https://www2.ed.gov/about/offices/list/ocr/complaintintro.html

SORN: https://www2.ed.gov/notices/sorn/18-08-01a_031504.pdf

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

A written consent form is available for individuals and is published online at the following address: https://www2.ed.gov/about/offices/list/ocr/edlite-consentform.html

4. Information Sharing

4.1. Will information be shared internally with other ED organizations, if so, which ones?

OCR does not generally share the PII in its files with other ED organizations. At times, OCR may need to collaborate with ED’s Office of the General Counsel (OGC) to resolve difficult legal issues of first impression and during this process OCR may share the facts of a case without, generally, sharing PII. OCR also sometimes must respond to inquiries from ED’s Office of the Inspector General (OIG) about one of OCR’s investigations, and during this process OCR may share the facts of a case without, generally, sharing PII. In response to inquiries from Congress, OCR also shares some case files with ED’s Office of Legislation and Congressional Affairs (OLCA), so that they may in turn be shared with Congress, but OCR has already removed PII from the files before doing so.
4.2. What information will be shared and with whom?

See response above.

4.3. 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?

See response above.

External

4.4. Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)?

Yes, if it requests a copy of the file. It is also necessary for OCR to disclose some information in order to investigate a complaint of discrimination.

4.5. What information will be shared and with whom?

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., enforcing Federal Statutes. Possible disclosures include:

- Disclosure to Congress, other agencies, or the public
- Disclosure to recipients of Federal financial assistance, witnesses, or consultants
- Disclosure for use by other law enforcement agencies
- Enforcement disclosure
- Litigation and Alternative Dispute Resolution (ADR) disclosures
- Freedom of Information Act advice 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.

There will be no sharing of information for purposes outside of the above disclosure requirements or for anything other than the primary purpose(s) of collecting the information. Any contractor responsible for the operations of the CAMS is held to the
privacy and security requirements of the Department in the handling of information collected through the systems.

4.6. What is the purpose for sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

OCR must comply with Federal laws, including the Freedom of Information Act, and this requires OCR to disclose certain information as requested. However, PII is redacted before the information is shared.

As stated above, OCR also may have to share PII with a recipient of Federal financial assistance in order to investigate a claim that the recipient has violated one of the civil rights laws that OCR enforces.

4.7. How is the information accessed and used by the external entity?

External entities cannot access CAMS. Only OCR employees and CAMS contractors have access to CAMS, and it is OCR employees who access information stored in CAMS and, if warranted in particular situations, who share that information with external entities.

During an audit by the Department’s Office of the Inspector General (OIG) (Control Number ED-OIG/A19N0002, which was concluded in December 2015), OCR allowed OIG to have limited access to CAMS.

4.8. If the project is using the information for testing a system or for training/research purposes, what controls are in place to minimize the risk and protect the data?

Only OCR employees and CAMS contractors have access to CAMS. In order to access CAMS, employees and CAMS contractors must sign in to the system using their unique passwords. The application access list is controlled by the system owner and the network access is established by the OCIO contractor managing the network.

4.9. Does the system use “live” PII for the development or testing of another system? If so, please explain.

No, but live PII is used for testing of CAMS, which only CAMS approved users have access.
4.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency?

There is no Computer Matching Agreement, Memorandum of Understanding or other type of approved sharing agreement with another agency.

4.11. Does the project place limitations on re-disclosure?

The CAMS doesn’t place limitations on re-disclosure. However, there is attorney-client privilege that restricts the sharing case information.

5. Redress

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

By filing a request pursuant to a Freedom of Information Act (FOIA), a person can obtain a written copy of a case file. However, even in these circumstances PII is generally redacted prior to release of the case file. Individuals cannot access their information directly from CAMS.

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

When OCR opens a complaint for investigation, OCR sends a Letter of Notification to both the complainant and the recipient that is the subject of the complaint. An individual may contact OCR, either in writing or by telephone, to relate what he or she believes is inaccurate or erroneous information, particularly if it is in relation to PII. However, OCR is an independent law enforcement agency that gathers data from all parties to a dispute and an individual may not agree with some of this data.

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

OCR provides information of its Investigatory Use of Personal Information on its Complaint Form (pages #11-12). OCR also informs complainants that a signed, written consent form may be required in order for OCR to proceed with an investigation.

---

5 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed onto Section 7. Safeguards.
There is also a published Privacy Act Notice, SORN #18-08-01, Complaint Files and Log.

6. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO

6.1. 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, the ISSO works in accordance with the Office of Chief Information Office’s Information (OCIO) Assurance Team. OCR implements the security and privacy protocols as directed.

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

Only OCR employees and CAMS contractors have access to CAMS. In order to access CAMS, employees and CAMS contractors must sign in to the system using their unique passwords. The application access list is controlled by the system owner and the network access is established by the OCIO contractor managing the network. This method creates a ticket and a mechanism to track the user’s access into the system.

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

The network access is granted through a ticket system by the system owner. The system owner generates a password for the system and the user’s network credentials are used to authenticate the user along with the system password generated by system owner.

The physical safeguards are the data center is located off site and no direct access by the system owners or users.

6.4. Is an Authority to Operate (ATO) required? Has one been granted?

An ATO is required and OCR has authorized its ATO.

6.5. Is the system able to provide an accounting of disclosures?

No,
7. Auditing and Accountability

7.1. How does the system owner ensure that the information 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. Additionally, all staff are required to complete mandatory cyber security training and the management of sensitive data including PII.

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

CAMS can be accessed only by employees and CAMS contractors; these employees and contractors have been subject to security clearances and are required to undergo regular trainings, including on the subject of protecting PII. In order to access information in CAMS, staff and contractors must sign in with their unique identifiers and their activities are tracked. Furthers, CAMS is located inside the Department’s firewall to help prevent access by outsiders.