Privacy Impact Assessment (PIA)
for the

Case and Activity Management System (CAMS)

May 20, 2022

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: Jacqueline.Lumford@ed.gov

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 U.S. Department of Education's (Department) Office for Civil Rights (OCR) utilizes the Case and Activity Management System (CAMS) which contains two in-house developed applications: the Case Management System (CMS) and the Activity Management System (AMS). CAMS utilizes the commercial off-the-shelf software, Open Text eDOCS Document/Record Management System (DM/RM). CMS maintains, manages, and tracks complaints, directed inquiries, and technical assistance activities carried out by OCR's regional offices. The AMS allows for the management of non-case related business activities by the OCR Program Legal Group (PLG). The DM/RM stores, maintains, and integrates documents/records to permit end-to-end electronic processing of cases and activities. In addition, the DM/RM houses a central repository for documents on OCR policy, compliance standards, case work tools, technical assistance tools, and training materials to be used by all OCR components.

CAMS, a combination of an internal-facing website, portal, and database, supports OCR's mandate to enforce Federal statutes that prohibit discrimination by recipients of Federal financial assistance from the Department. 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 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.

CAMS manages OCR caseloads and provides reporting information used in congressional reports, budget requests, Freedom of Information Act (FOIA) requests, and requests from other government agencies and the general public. CAMS also manages non-case related business activities including, but not limited to, legal and policy guidance, case support, data collection and analysis, information dissemination, and program coordination with other Department components and Federal agencies, as well as legal documents on case-related matters, research, reports, regulations, legislation, briefing materials, training materials, and manuals through the DM/RM software.

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

OCR collects, uses, maintains, and shares PII for the purpose of conducting its case processing work in order to support OCR's mandate to enforce Federal statutes that prohibit discrimination by recipients of Federal financial assistance from the Department. OCR uses CAMS to manage record-keeping on the investigation of complaints, proactive investigations, and other civil rights activities more effectively and efficiently.

While investigating a complaint, OCR staff collects: the complainant's name, address, and telephone number; the specific allegations of discrimination at issue; and data collected from complainants, recipients, and other sources. OCR staff then input this information into CAMS to assist with evaluating, investigating, and resolving complaints. In addition, OCR also may collect and store data in CAMS from recipients and other sources in connection with conducting directed investigations and compliance reviews.

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

The PIA is being updated as part of the required biennial review.

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.

[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

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.

OCR enforces six Federal civil rights statutes:
Title VI of the Civil Rights Act of 1964, prohibiting discrimination on the basis of race, color, and national origin is prohibited by; Title IX of the Education Amendments of 1972, prohibiting discrimination on the basis of 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 the basis of disability; the Age Discrimination Act of 1975, prohibiting discrimination on the basis of age; and the Boy Scouts of America Equal Access Act of 2001, prohibiting the denial of equal access or a fair opportunity to meet with 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.

In addition, OCR collects and maintains PII pursuant to the Family Education Rights and Privacy Act, 20 U.S.C. §§ 1232g(b)(1) and 1232g(b)(3).

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

The records in this system are indexed by and retrievable by any data element in any populated data field, including the name of the complainant, the complaint number, the name of the entity against which the complaint was filed, the basis for the alleged discrimination, and the stage of case processing.

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

The SORN, entitled the "Complaint Files and Log'' (18-08-01), 83 FR 12571, was published in the Federal Register on March 22, 2018.

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.

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?

[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

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.

PII elements collected, used, disseminated, and maintained within CAMS include:

- Names, addresses, and telephone numbers of complainants, complaint allegations, and, depending on the details of the case, the age, race, and sex of alleged victims and other results of investigations.
- 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 emails or other written communications.
- Investigator and attorney memoranda.
- Interview notes or transcriptions and witness statements.
- 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.
- 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?

Yes

Depending upon the type of complaint and subsequent investigation, the minimum amount of PII is collected in order to fully complete an investigation and render a decision.

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

Any member of the public that files a civil rights complaint with the Department, including students, parents, teachers, and community advocates. Information from other individuals referenced as part of an investigation or complaint, such as witnesses, could also be collected.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Initial submissions of complaints can be submitted through 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. During an investigation, PII can be collected from stated sources through oral interviews, paper documents or USB drives sent by hand delivery or through physical mail, faxes, and/or email. For appeals, complainants fill out the appeal form.

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?

The complainant submits information directly into the system through the website or through a fillable 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.

During an investigation, staff assigned to the case validate or confirm information through interviews, email communications, and comparison of various documents. Staff communicate with complainants and recipients as needed during the course of investigations.

Use

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

OCR investigations typically focus on the treatment of individuals and often focus on how that treatment may or may not have varied from the treatment of other similarly situated individuals. To investigate, OCR must: understand an individual's status and confirm the particulars of the treatment received; identify individuals who are similarly situated; determine how those similarly situated individuals were treated; and examine a recipient's explanation for any differences in treatment. OCR investigations require

[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.

review of recipient files in areas that necessarily include PII, such as sexual harassment investigations, issuance of discipline, and services and accommodations for disability.

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

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

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 Notice found 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.

In addition, OCR provides notice to individuals during an investigation about the collection of PII prior to uploading any such information to CAMS in numerous ways, including the following:

- OCR's Case Processing Manual, Sections 101 and 703, available on OCR's website at https://www2.ed.gov/about/offices/list/ocr/docs/ocrcpm.pdf
- OCR's Notice of Witness Rights, which is shared with witnesses before interviews, pursuant to the Case Processing Manual, Section 702, and can be found at http://www2.ed.gov/about/offices/list/ocr/docs/witness-notice-mw.pdf
- Information About OCR's Complaint Processing Procedures, in a section entitled "Investigatory Use of Personal Information," which is found on OCR's website at https://www2.ed.gov/about/offices/list/ocr/docs/complaints-how.pdf
- How the Office for Civil Rights Handles Complaints, in a section entitled "Investigatory Use of Personal Information," which is found on OCR's website at https://www2.ed.gov/about/offices/list/ocr/complaints-how.html
- OCR Complaint Consent Form, which is found on OCR's website at https://www2.ed.gov/about/offices/list/ocr/edlite-consentform.html

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

See the links provided above under question 4.1.

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?

When it is necessary to disclose the identity of the complainant to the recipient and witnesses in order to resolve the complaint, OCR will require written consent before proceeding. The complainant will be informed that the complaint will be dismissed if written consent is necessary in order to resolve the complaint and is not received within 20 calendar days of the date that OCR requests the consent form from the complainant. The signed consent form may be submitted to OCR by mail, fax, electronic mail or in person. If OCR does not receive a signed written Consent Form, and it is necessary in order to resolve the complaint, the complaint will be dismissed and the complainant so informed in writing. A complainant filing on behalf of or pertaining to another person is

responsible for securing any necessary written consent from that individual, including when a parent files for a student over the age of 18 or one who becomes 18 while the complaint is under investigation or in monitoring. Where the person is a minor (under the age of 18) or a legally incompetent adult, the consent form must be signed by that person's parent or legal guardian. Parental or legal guardian consent may not be required for persons under the age of 18 if they are emancipated under State law.

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

PII may be shared with different internal offices such as the Office of the General Counsel (OGC), the Office of the Inspector General (OIG), or the Office of Legislative and Congressional Affairs (OLCA).

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

☐ N/A

OCR does not generally share the PII in its files with other Department organizations. At times, however, OCR may need to collaborate with OGC to resolve litigation involving complainants or recipients or difficult legal issues. OCR also sometimes must respond to inquiries from OIG about OCR investigations, and during this process OCR may need to share the facts of a case. OLCA coordinates inquiries from and responses to members of Congress; in response to an inquiry from a member of Congress about a case, so long as that member has consent signed by a party to the case (complainant or parent/legal

guardian), OCR may share limited case information with OLCA for the purpose of conveying such information to the member of Congress.

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.

Yes

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

Information includes: complainant's name, address, and telephone number; the specific allegations of discrimination at issue; and other facts gathered in investigation of the allegations.

Possible disclosures include:

- Recipients of Federal financial assistance, witnesses, or consultants
- Law enforcement agencies
- Litigation and alternative dispute resolution (ADR)
- Department of Justice (DOJ)
- Members of Congress
- Contractors

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

☐ N/A

OCR shares PII with the DOJ as necessary for DOJ to coordinate OCR's civil rights work and for the two organizations to work together on certain investigations. Similarly, other agencies sometimes delegate to OCR their authority to conduct civil rights investigations, in which case OCR may share the result of such an investigation with the delegating agency. When OCR receives a complaint over which it does not have jurisdiction, it may share the complaint, including PII, with another enforcement agency that does have jurisdiction. OCR shares PII with recipient and witnesses as necessary in order to obtain appropriate records and information during ongoing OCR investigations

[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.

and may share PII with consultants assisting OCR to conduct investigations. Where OCR is pulled into litigation by a complainant or recipient, OCR may be forced to share PII with a court or to pursue ADR. When Congressional members pose inquiries on behalf of constituents who are complainants or recipients, OCR discloses PII if the member of Congress provides to OCR a consent to share PII signed by the complainant or parent/legal guardian.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

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

☐ N/A

No

The Secretary of Education has exempted by regulations the Complaint Files and Log record system, which is also exempt from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552(k)(2) (civil enforcement):

(1) 5 U.S.C. 552a(c)(3), regarding access to an accounting of disclosures of records.

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

☐ N/A

External entities cannot access CAMS. Only authorized OCR employees and contractors have access to CAMS. Both have access to information stored in CAMS and, if warranted in particular situations, share that information with external entities. PII typically is shared via physical letters and/or encrypted email.

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

No

The sharing of information is pursuant to the routine uses maintained in the Complaint Files and Log (18-08-01) SORN.

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

☐ N/A

No

6. Redress

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

This system is exempted from 5 U.S.C. 552a(e)(4)(H) pursuant to 34 CFR 5b.11(c)(2)(iii).

OCR generally processes an individual's request for "their information" as a request under both the Privacy Act and FOIA, absent further clarification. Pursuant to the Privacy Act, individuals can obtain unredacted documents in a system of records maintained under their names or other PII, so long as a requesting individual signs a Privacy Act Request Form swearing under penalty of perjury about the truthfulness of his or her identity. Individuals also can file FOIA requests seeking case files that incidentally may contain their PII, in which case, if disclosure otherwise is appropriate under FOIA, they will be given documents unredacted as to their own PII and redacted as to other individuals' PII. Individuals cannot access their information directly from CAMS.

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

This system is exempted from 5 U.S.C. 552a(e)(4)(H) pursuant to 34 CFR 5b.11(c)(2)(iii).

There is no formal procedure for correcting information. As stated above, OCR conducts ongoing efforts to collect, and corroborate information, consistent with OCR's Case Processing Manual, which States that case planning is to be conducted throughout the life of every case to ensure high quality decisions, and planning decisions will be adjusted as necessary to take into account information obtained during case processing. OCR's resolution letters and its Case Processing Manual inform parties about appeal rights.

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

This system is exempted from 5 U.S.C. 552a(e)(4)(G) pursuant to 34 CFR 5b.11(c)(2)(iii).

Throughout the course of case evaluation and investigation, OCR communicates with complainants and recipients to obtain and confirm information. For example, when OCR opens a complaint for investigation, OCR sends a Letter of Notification to both the complainant and the recipient about the subject of OCR's investigation. At any point during OCR's communications, an individual may contact OCR to relate what he or she believes is inaccurate or erroneous information, including 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. If parties disagree with OCR determinations as laid out in resolution letters, there is an appeal process.

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 server facilities. The system is only accessible and available to authorized Department employees and contractors utilizing various authentication mechanisms including usernames and passwords. The system also limits data 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 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.

File folders containing non-digital information in the system are kept in locked storage rooms. Access to offices in which storage rooms are located is restricted to OCR staff and authorized visitors.

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.

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

The following tasks are performed to safeguard CAMS information:

- Monthly vulnerability scans performed
- Annual contingency plan test performed
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team
- Annual updates to system security documents
- Annual mandatory cybersecurity and privacy training for employees

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 Information System Security Officer performs challenge tests using invalid usernames and passwords annually and 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.

Staff are trained directly by the system owner on the requirements of the Case Processing Manual, and each regional office maintains a system of review to ensure that case work and associated communications are conducted in conformity with the Case Processing Manual, including issuing letters with appropriate language about FOIA and appeal rights, and advising interviewees beforehand about their rights under FOIA and the Privacy Act. This ensures PII is used by all employees in accordance with what is documented in this PIA.

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. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff

at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.

Another privacy risk is related to data integrity. Because CAMS maintains information and data that OCR collects from various parties at different points in time, CAMS may reflect PII that no longer is accurate or that pertains to third parties. OCR mitigates the risk of inaccuracy by actively seeking to corroborate the information that it collects during the course of an investigation, and by noting in CAMS when a case is closed, thereby indicating that information no longer is being updated and instead reflects an historical record. Privacy risks for complainants and third parties are mitigated because OCR tracks its cases by docket number, not complainant name. Further, as noted above, CAMS can be accessed only by employees and CAMS contractors, who have been subject to security clearances and are required to undergo regular trainings, including about protecting PII, and whose accessing of specific documents is tracked by the CAMS system.