

PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Peace Corps Case Adjudication Tracking System (PCCATS)

Managing Office: Office of Safety and Security (OSS)

Privacy Impact Assessment (PIA) Approval date: March 27, 2023

1. Is this a new or revised electronic information system?

This is a revised PIA.

If any question does not apply, state not applicable (N/A) and explain why.

2. Identify who the Personally Identifiable Information (PII) is collected from:

Members of the public, including Peace Corps Volunteer applicants and interns

Federal employees/federal contractors/Peace Corps Volunteers

Both members of the public and Peace Corps personnel

3. Legal Authority. Cite the legal authorities that permit and authorize the collection of this information by this IT system.

The Peace Corps Act, 22 U.S.C. 2501 et seq.; Executive Order (EO) 9397, as amended; EO 10450; EO 13869, Homeland Security Presidential Directive-12; Office of Management and Budget Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors."

4. Purpose. Explain the purpose of the system (e.g., nature and source).

Peace Corps Case and Adjudication Tracking System (PCCATS) supports the following primary interrelated functions: Electronic tracking of personnel security data, pre-investigation screening and reviews, submission to the Office of Personnel Management and to the Defense Counterintelligence and Security Agency (DSCA) of the Electronic Questionnaires for Investigations Processing (e-QIP) for initial or re-investigations, adjudication of investigation, managing security clearance evaluations and reporting.

5. List all forms of Personally Identifiable Information (PII) that is collected, maintained, or disseminated.

- Last name, first name, middle name, also known as title, suffix
- Personal home address, zip code, personal phone number, work number
- Biometrics, to include height, weight, hair color, eye color, sex.

- Social Security Number (full)
- Date of birth
- Birth city, birth state, birth country
- Country/countries of citizenship
- Citizenship identification information (passport number, visa number, alien registration number, etc.)
- Residence information/history
- Selective Service information
- Employment history
- Education history
- Credit report and financial record
- Background investigation and national security clearance information/record
- Resume
- Family member information
- Driver's license number
- Marital status/ history
- Police record and law enforcement information,
- Non-criminal court action information
- Educational information
- Illegal drug use history
- Alcohol Use history
- Personal reference information
- Foreign contacts
- Foreign travel history
- Foreign business, professional activities
- Protected Health Information, psychological and emotional history
- Official Personnel Folder

6. Why is PII being collected (e.g., to determine eligibility)? Does the IT system collect PII directly from individuals, or from another system?

PII is collected for the personnel security process to determine eligibility for federal employment in accordance with government wide standards established by OPM, DCSA, and the Department of Defense (DOD). The process includes credentialing, suitability/fitness determination, national security determination, reciprocity review, reinvestigation review, continuous evaluation and self-reporting requirement. The system does not collect PII directly from the applicant/subject or directly from another system (system-to-system). An Office of Human Resources (OHR) member and/or a Personnel Security specialist collects and enters all information in PCCATS from the Optional Form (OF) 306 and other initial job application records by manually keying in or manually uploading it. OHR personnel manually enter information from the IT system Career Connector for new personnel.

7. Sharing and Disclosure.

a. Will the PII from this system be shared with another agency? If yes, list the agency, all types of PII that is shared, and why this is shared outside our agency.

PCCATS is unable to share PII with another agency at this time.

The system has the ability to connect with DCSA and the Department of Defense (DOD)'s adjudication system in order to receive, submit and update electronic investigation files and records. However, the system does not have this function at this time. OPM and DCSA have instructed that all agencies must be able to receive electronic investigation files through a database, such as PCCATS.

b. Is the sharing pursuant to a Memorandum of Understanding, Computer Matching Agreement (CMA), or other type of approved sharing agreement with another agency?

No. This is not applicable.

8. Notice of the collection of information.

Applicants/subjects are notified that their PII will be collected when a tentative offer of employment is issued by OHR. If the offer is accepted by the applicant, then the individual is instructed to complete security paperwork required to initiate the personnel security process. OF-306, a primary source of information, also provides a Privacy Act Statement (PAS).

a. Do individuals have the opportunity to object or to consent to the particular use of their PII prior to collection?

Yes No

b. If "Yes," describe the Privacy Act Statement (PAS) or notice provided to the individual prior to collection of his or her information. If "No," state the reason why individuals cannot give or withhold their consent. Identify if this is not applicable because information is obtained from an existing information system or source.

All applicants/subjects in the personnel security process are required to complete a Declaration of Federal Employment form, OF-306, which includes a PAS. Applicants sign this form with consent before it is submitted for review. No PII is collected until OHR receives the OF-306 form and other consent forms, such as the credit release form. If a new background investigation is required, applicants are required to complete a Questionnaire for Public Trust Positions or Questionnaire for National Security Position. Before this questionnaire can be closed as complete and released to OSS for review, the applicant/subject must sign the Authorization for Release of Information section.

c. List any Peace Corps form(s) or federal form(s) used to collect PII for this system. Each PC form must have a Privacy Act Statement.

OF-306, Declaration for Federal Employment.

d. Provide the OMB Control number and the agency number for the collection if this collection is covered by the Paperwork Reduction Act (PRA).

OF-306, Declaration of Federal Employment: OMB number 3206-0182

9. Security.

a. What administrative, technical, and physical security safeguards/controls are in place to protect the PII?

The administrative, technical, and physical privacy risks include unauthorized access, unauthorized disclosure, and a risk that the individuals whose information is added to PCCATS. There are administrative, physical security, and technical safeguards in place to mitigate these risks.

Administrative Controls: Only authorized Security personnel and OHR administrators have restricted access to the office, the designated system, and its information based on a need-to-know basis to fulfill their official duties. Senior administrators assign user roles within OSS and OHR to limit access to only those who have an official need to know to perform their official duties. Authorized users are trained in the proper handling of PII and of their official responsibilities under the Privacy Act and Peace Corps technical governance for the rules of behavior.

Technical controls: PCCATS is restricted only to a designated group within OSS and OHR. Access control requires the use of Single-Sign-On (SSO). Users are authenticated using approved/assigned username and password into the system. The PCCATS administrator controls user access to system functionality and data by assigning system roles with access permissions.

b. Has a system security plan been completed for the information system?

Yes, a system security plan was completed for the system in 2022. The system is undergoing a continuous monitoring assessment scheduled for March 2023.

10. Privacy Act System of Records. Identify the System of Record Notice (SORN) that covers this IT system, or state if a SORN will be created under the Privacy Act, 5 U.S.C. 552a.

PC-13, Personnel Security Records; OPM/GOVT-1, General Personnel Records.

11. Records Retention and Disposition. Identify the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system, or for the records maintained in the system, as well as the record retention instructions.

DAA-GRS-2017-0006-0024 and 0025 / GRS 5.6, item 180; DAA-GRS-2017-0006-0025 / GRS 5.6, item 181; DAA-GRS-2017-0006-0022 / GRS 5.6, item 170; DAA-GRS-2017-0006-0023 / GRS 5.6, item 171; DAA-GRS-2017-0006-0026 / GRS 5.6, item 190