

information, the Secretary will establish an electronic docket for the proceeding if the Secretary has not already established an electronic docket.

Information about applying for a digital ID certificate is available on the NRC's public website (<https://www.nrc.gov/site-help/e-submittals/getting-started.html>). After a digital ID certificate is obtained and a docket is created, the participant must submit adjudicatory documents in the Portable Document Format. Guidance on submissions is available on the NRC's public website (<https://www.nrc.gov/site-help/electronic-sub-ref-mat.html>). A filing is considered complete at the time the document is submitted through the NRC's E-Filing system. To be timely, an electronic filing must be submitted to the E-Filing system no later than 11:59 p.m. ET on the due date. Upon receipt of a transmission, the E-Filing system time-stamps the document and sends the submitter an email confirming receipt of the document. The E-Filing system also distributes an email that provides access to the document to the NRC's Office of the General Counsel and any others who have advised the Office of the Secretary that they wish to participate in the proceeding, so that the filer need not serve the document on those participants separately. Therefore, applicants and other participants (or their counsel or representative) must apply for and receive a digital ID certificate before adjudicatory documents are filed in order to obtain access to the documents via the E-Filing system.

A person filing electronically using the NRC's adjudicatory E-Filing system may seek assistance by contacting the NRC's Electronic Filing Help Desk through the "Contact Us" link located on the NRC's public website (<https://www.nrc.gov/site-help/e-submittals.html>), by email to MSHD.Resource@nrc.gov, or by a toll-free call at 1-866-672-7640. The NRC Electronic Filing Help Desk is available between 9 a.m. and 6 p.m., ET, Monday through Friday, except Federal holidays.

Participants who believe that they have good cause for not submitting documents electronically must file an exemption request, in accordance with 10 CFR 2.302(g), with their initial paper filing stating why there is good cause for not filing electronically and requesting authorization to continue to submit documents in paper format. Such filings must be submitted in accordance with 10 CFR 2.302(b)-(d). Participants filing adjudicatory documents in this manner are responsible for serving their documents on all other participants. Participants granted an exemption

under 10 CFR 2.302(g)(2) must still meet the electronic formatting requirement in 10 CFR 2.302(g)(1), unless the participant also seeks and is granted an exemption from 10 CFR 2.302(g)(1).

Documents submitted in adjudicatory proceedings will appear in the NRC's electronic hearing docket, which is publicly available on the NRC's public website (<https://ehd.nrc.gov>), unless otherwise excluded pursuant to an order of the presiding officer. If you do not have an NRC-issued digital ID certificate as previously described, click "cancel" when the link requests certificates and you will be automatically directed to the NRC's electronic hearing docket where you will be able to access any publicly available documents in a particular hearing docket. Participants are requested not to include personal privacy information such as social security numbers, home addresses, or personal phone numbers in their filings, unless an NRC regulation or other law requires submission of such information. With respect to copyrighted works, except for limited excerpts that serve the purpose of the adjudicatory filings and would constitute a Fair Use application, participants should not include copyrighted materials in their submission.

Authority: 42 U.S.C. 2011 *et seq.*

Dated: September 22, 2026.

For the Nuclear Regulatory Commission.

Jane Marshall,

Director, Division of Decommissioning, Closure, Analysis, and Financial Oversight, Office of Nuclear Material Safety and Safeguards.

[FR Doc. 2026-19649 Filed 9-24-26; 8:45 am]

BILLING CODE 7590-01-P

PEACE CORPS

Privacy Act of 1974; System of Records

AGENCY: Peace Corps.

ACTION: Notice of a new system of records.

SUMMARY: As required by the Privacy Act of 1974, as amended, and the Office of Management and Budget (OMB) Circulars A-108 and A-130, the Peace Corps Office of Planning and Performance (OPP) is issuing a public notice of its new system of records Peace Corps Customer Relationship Management (Agency CRM) System of Records ("PC 38"). The Office of Planning and Performance (OPP) manage and utilizes a management database system to monitor, track, and analyze all interactions with prospective

and current Peace Corps applicants from the time they visit the agency website, its social media pages, apply for volunteer service and their volunteer activity throughout their volunteer service. This system of records contains information on members of the public who become leads and visit the Peace Corps websites, social media pages and apply to become applicants as well as those who are current volunteers and through completion of volunteer service.

DATES: Submit comments on or before October 26, 2026 This new system will be effective October 26, 2026.

ADDRESSES: Send written comments, identified by the docket number and title, to the Peace Corps, ATTN: James Olin, Government Information Specialist, Office of Compliance and Risk, 1275 First Street NE, Washington, DC 20526, or by email at pcf@peacecorps.gov. Email comments must be made in text and not in attachments.

FOR FURTHER INFORMATION CONTACT: James Olin, Government Information Specialist, Office of Compliance and Risk, 1275 First Street NE, Washington, DC 20526; pcf@peacecorps.gov; or 202-692-2507.

SUPPLEMENTARY INFORMATION: Section 5 of the Peace Corps Act of 1960, as amended (codified as 22 U.S. Code § 2504) authorizes the recruitment and enrollment of Peace Corps volunteers. Under this section, the agency is granted the authority to enroll qualified United States citizens and nationals for service abroad, and the operational power to select, train, and manage volunteers. As part of the Recruitment Analytics and Identity Resolution Initiative (RAIRI) the agency will sync anonymized Client IDs, currently assigned to leads, with the non-anonymized lead records stored in Peace Corps' customer relationship management database, and with applicant tracking internal systems, PCrm, Volunteer Applicant Tracking System (DOVE) and Medical Applicant Exchange System (MAXx).

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), which governs the collection and protection of personal information by federal agencies, the Peace Corps is establishing a new system of records to manage personal information from members of the public who become leads and applicants who interact with Peace Corps' website, social media and volunteer recruitment activities. The system will also track applicant responses to recruitment methods, progress through the application process, and completion of volunteer service. This system will connect lead and applicant data,

training, and volunteer service to optimize recruitment strategies and assess applicant and volunteer retention and volunteer program outcomes. It will also integrate internal platforms, including PCrm, Volunteer Information Database Application (VIDA), Security Incident Management System (SIMS), Peace Corps Recruitment and Marketing (PCrm), Returned Peace Corps Volunteer Outreach (RPCV Outreach), the Director's Correspondence Log, MAXx and DOVE, to track applicant communications with staff regarding applications, medical clearance, and program success. This initiative underscores the agency's commitment to safeguarding personal information and improving operational effectiveness.

SYSTEM NAME AND NUMBER:

Peace Corps Customer Relationship Management System of Records (Agency CRM), PC-38.

SECURITY CLASSIFICATION:

Moderate.

SYSTEM LOCATION:

Records are maintained in an electronic form on a Software as a Service (SaaS) platform under contract with the Peace Corps, Office of Information Systems, 1275 First St. NE, Washington, DC 20002.

SYSTEM MANAGER(S):

The Director of Office of Planning and Performance, and the Chief Information Officer, Office of Information Systems, Peace Corps, 1275 First St. NE, Washington, DC 20002.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 4 of the Peace Corps Act of 1961, as amended (22 U.S.C. 2504; the Privacy Act of 1974, 5 U.S.C. 552a, and Peace Corps Manual Section (MS) 129: Office of Information Systems and MS 542: Information Security Program.

PURPOSE(S) OF THE SYSTEM:

The Peace Corps will utilize this system to effectively track, monitor, and analyze interactions with both potential and current applicants and volunteers. The primary purpose of the system is to support the recruitment and retention process, and gain insight into the best practices in marketing, recruitment, onboarding, retention, and volunteer matriculation throughout the entire duration of volunteer service. By collecting, managing, and analyzing the aggregation of these records and data points, the Peace Corps aims to improve operational efficiency, maintain accurate documentation, and uphold

best practices for volunteer recruitment, engagement and retention.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system covers members of the public who interact with the agency's social media and website, and are assigned a client ID through Google Analytics; applicants, trainees, and volunteers of the Peace Corps; authorized users who access Peace Corps computer networks, enterprise servers, or certain agency database systems related to applicants, trainees and volunteers; and personnel responsible for maintaining records, privacy and security, and software applications within these network systems. In addition, this system includes individuals who recruit prospective applicants and volunteers, as well as those who analyze applicant and volunteer data for the purposes of supporting recruitment, onboarding, retention, and program evaluation.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Office of Information Systems is responsible for maintaining the category of Peace Corps Customer Relationship Management System of Records. This system includes information pertaining to members of the public who become leads, applicants seeking to become volunteers, trainees, volunteers, and returned Peace Corps volunteers. The system maintains additional records after the leads become applicants, and volunteers. These records may include personal identifiers such as name, email address, home address, telephone number, Social Security Number, demographic information (including race, ethnicity, disabilities, etc.), birth date, marital status, fingerprints, citizenship status, government-provided identification documents and the Client ID provided by Google Analytics. The records may also contain detailed information about applicants, trainees and volunteers that include:

- Their application to become a volunteer (e.g., reason for applying, educational history, employment history, military history, prior community service activities, criminal history, medical history, skills, certifications, and references, etc.).
- Peace Corps service history and experience (e.g., descriptions of activities, performance reviews, disciplinary concerns, health related to volunteer service, reasonable accommodation, leave requests, service-related travel and service training).
- Benefits (e.g., health benefits, stipends, loan forbearance).

- Emergency contacts and beneficiaries.

Additionally, the system contains program participant descriptions and information regarding recruitment program activities, as well as details about services received by volunteer participants. The records may also include information obtained after the completion of the volunteer program.

The records maintained in this system also cover several aspects of electronic communication and access within the Peace Corps. These include documentation of interoffice and internet email activity, such as the email addresses of both sender and receiver, the subject line, and the date and time each message was sent or received.

Additionally, the system tracks user activity on Peace Corps networks. Records include user identification, the date and time each user logs on or logs off, and any instances where access to unauthorized files or directories is denied. Internet access from Peace Corps computers is also recorded, capturing the internet Protocol (IP) address used, the specific sites accessed, and the corresponding date and time of each connection.

Further records relate to system access, documenting the user ID of individuals accessing the system, the date and time of access, and the processes being run on the system. Verification and authorization activities are also recorded, including details such as user IDs, passwords, usernames, titles, and agency affiliations, to ensure proper security and oversight of system access.

RECORD SOURCE CATEGORIES:

The Office of Information Systems is responsible for maintaining the record source of categories for the Peace Corps Customer Relationship Management System of Records. The source for information in the system comes from the individuals who provide their information or their representative. The information sources may also include authorized Peace Corps staff members, contractors, Peace Corps volunteers, and other individuals or entities associated with Peace Corps and the internal electronic platforms such as PCrm, Medical Applicant Exchange System (MAXx), Volunteer Applicant Tracking System (DOVE) and Google Analytics. Most records are generated internally from computer activity logs individuals covered by the system and management officials.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USERS:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, the Peace Corps may disclose all or a portion of the records or information contained in this system outside of the Peace Corps without the consent of the subject individual, if the disclosure is compatible with the purpose for which the record was collected, as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. Disclosure for Law Enforcement Purposes. Information may be disclosed to the appropriate Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the information indicates a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving entity.

B. Disclosure Incident to Requesting Information. Information may be disclosed to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, or to identify the type of information requested); when necessary to obtain information relevant to a Peace Corps decision concerning retention of an employee or other personnel action (other than hiring), retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit.

C. Disclosure to Requesting Agency. Information may be disclosed to a Federal, State, local, or other public authority of the fact that this system of records contains information relevant to the requesting agency's retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for part or all of the record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

D. Disclosure to Office of Management and Budget. Information may be disclosed to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A-19.

E. Disclosure to Congressional Offices. Information may be disclosed to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of the individual.

F. Disclosure for Litigation. Information may be disclosed for litigation purposes. Disclosure for these purposes may be made to the Department of Justice, or in a legal proceeding before a court, adjudicative body, or other administrative body before which the Peace Corps is authorized to appear. This disclosure may be made when: (1). In any legal proceeding, where pertinent, to which Peace Corps or the United States is a party before a court, tribunal or administrative body; (2). any employee of the Peace Corps in his or her official capacity with a need to know; (3). any employee of the Peace Corps in his or her individual capacity where the Department of Justice or the Peace Corps has agreed to represent the employee; or (4). when the Peace Corps determines that litigation is likely to affect the Peace Corps or any of its components and has an interest in such litigation, and the use of such records by the Department of Justice or the Peace Corps is deemed by the Peace Corps to be relevant and necessary to the litigation.

G. Disclosure to the National Archives. Information may be disclosed to the National Archives and Records Administration in records management inspections.

H. Disclosure to Contractors, Grantees, and Others. Information may be disclosed to contractors, grantees, consultants, or volunteers performing or working under a contract, service agreement, grant, cooperative agreement, job, or other activity for the Peace Corps and who have a need to have access to the information in the performance of their duties or activities for the Peace Corps. Recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. 552a(m).

I. Disclosures for Administrative Claims, Complaints, and Appeals. Information may be disclosed to an authorized appeal grievance examiner, formal complaints examiner, intake officer, equal employment opportunity specialist, investigator, arbitrator, or other person properly engaged in investigation or settlement of an administrative grievance, complaint, claim, or appeal filed by an applicant, employee, or volunteer applicant, invitees, trainee or volunteer, but only to the extent that the information is relevant and necessary to the proceeding. Agencies that may obtain

information under this routine use include, but are not limited to: the Office of Personnel Management, Office of Special Counsel, Federal Labor Relations Authority, U.S. Equal Employment Commission, the Foreign Service Grievance Board and Office of Government Ethics.

J. Disclosure to the Office of Personnel Management. Information may be disclosed to the Office of Personnel Management pursuant to that agency's responsibility for evaluation and oversight of Federal personnel management.

K. Disclosure in Connection with Settlement. Information may be disclosed in connection with settlement discussions regarding claims by or against the Peace Corps, including public filings with a court, to the extent that disclosure of the information is relevant and necessary to potential litigation or settlement discussions and except where court orders are otherwise required under Section (b)(11) of the Privacy Act of 1974, 5 U.S.C. 552a(b)(11).

L. Disclosure to U.S. Ambassadors. Information from this system of records may be shared with a U.S. Ambassador or their designated representative in any country where the Peace Corps operates, when such disclosure is necessary for the Ambassador to fulfill official duties, respond to formal inquiries, or address in-country matters within their area of responsibility.

M. To appropriate agencies, entities, and persons when (1) the Peace Corps suspects or has confirmed that there has been a breach of the system of records; (2) the Peace Corps has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, the Peace Corps (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Peace Corps' efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

N. Disclosure to another Federal agency or Federal entity, when the Peace Corps determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national

security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All records are stored electronically in a Federal Risk and Authorization Management Program (FedRAMP) Certified Class D (High) Software as a Service (SaaS) data backup and recovery solution cloud service offering. As a FedRAMP Class D (High) certified solution all records are protected according to federal guidelines. All electronically stored records are encrypted both at rest and in transit using FIPS 140–3 authorized encryption standards. The SaaS cloud service offering leverages a FedRAMP Certified Infrastructure as a Service (IaaS) as its primary hosting environment, a dedicated cloud IaaS for U.S Government workloads. Physical security controls to the system includes high security locks, reinforced doors, 24 hours security guard management, and PIV cards to access the room.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name, Client ID, email address, or other personal or unique identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in the Volunteer Information Database Application (VIDA) Records (will be cut off at the end of the fiscal year in which the Volunteer is separated or resigns. These records will be destroyed 6 years after cutoff.

Records in the Security Incident Management System (SIMS) Will be cut off when the final action is taken on a case or when the system is decommissioned. These records will be destroyed no sooner than 10 years after cutoff but a longer retention is authorized. Recruitment Records will be cut off at the end of the fiscal year. These records will be destroyed 6 years after cutoff.

The Returned Peace Corps Volunteers Career Link Database Master File will be cut off at the end of each calendar year. These records will be destroyed 6 years after cutoff.

The Executive Correspondence Log will be cut off at the end of each presidential administrative term. The records will be transferred to the National Archives 20 years after the end of the presidential administration.

The Database of Volunteer Experience (DOVE) will be cutoff at the end of the fiscal year in which the final action is taken on the application. These records will be destroyed 6 years after cutoff.

The records in MAXx will be cutoff upon the Close of Service (COS) or termination of the Peace Corps Volunteer. These records will be destroyed 50 years after cutoff.

The Applicant Medical Case Files will be destroyed 7 years after either a final decision is rendered for a rejected applicant or Close of Service for a successful applicant.

Records in the Volunteer Reporting and Grants (VRG) will be destroyed 10 years after the final action is taken if the Applicant is successful. The records will be destroyed 3 years after the final action is taken if the Applicant is unsuccessful.

Records in the Peace Corps Volunteer Database Management System (PCVDBMS) will be transferred to the National Archives on an annual basis.

Peace Corps Customer Relationship Management System of Records is currently unscheduled and no data is authorized for destruction until the National Archives and Records Administration approves a disposition schedule.

Google Analytics retains Client IDs and associated data for a maximum of 26 months before deletion.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The Peace Corps safeguards records in this system in accordance with applicable laws, rules, and policies to protect personally identifiable information against unauthorized access or disclosure. Specifically, the agency's security and privacy controls comply with NIST 800–53, rev. 5—Security and Privacy Controls for Federal Information Systems and Organizations. The Peace Corps has imposed strict controls to minimize such risks. Administrative safeguards include but are not limited to: access to the information in this system is limited to authorized personnel with official duties requiring access, and whose roles have been authorized with such access permissions. All such individuals receive the appropriate privacy and cybersecurity training on an annual basis.

The physical controls in place include the servers storing electronic data are located offsite in a locked facility with access limited to authorized personnel. The servers are maintained in accordance with a government contract that requires adherence to applicable laws, rules, and policies on protecting individual privacy. Computerized records are safeguarded in a secured environment. Security protocols meet the promulgating guidance as established by the National Institute of

Standards and Technology (NIST) Security Standards from Access Control to Data Encryption and Security Assessment and Authorization and Peace Corps' privacy and security policies.

The technical controls in place include multiple firewalls, system access, encrypted data at rest, encrypted data in motion, periodic vulnerability scans to ensure security compliance, and security access logs. Access is restricted to specific authorized Peace Corps individuals who have internet access through work on computers using Personal Identity Verification (PIV). Individual users can only access records with the proper pre-approved accreditation. Physical security measures include but are not limited to the use of data centers which meet government requirements for storage of sensitive data.

RECORD ACCESS PROCEDURES:

Any individual who wants access to his or her record should make a written request to the System Manager. Requesters will be required to provide appropriate identification, such as a driver's license, employee identification card, or other authorized identifying documentation. Additional identification may be required in some instances. Complete Peace Corps Privacy Act procedures are set out in 22 CFR part 308.

CONTESTING RECORD PROCEDURES:

Individuals seeking to challenge the contents of a record after its submission to the system must submit a written request to the system manager. The request should include sufficient identification, such as a driver's license, employee identification card, or other official documentation; in certain cases, additional identification may be required. Requests for correction or amendment must clearly specify the record in question and the desired corrective action. For comprehensive guidance, refer to the Peace Corps Privacy Act procedures outlined in 22 CFR part 308.

NOTIFICATION PROCEDURES:

See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Dated: September 23, 2026.

James Olin,

Government Information Specialist.

[FR Doc. 2026–19684 Filed 9–24–26; 8:45 am]

BILLING CODE 6051–01–P