PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym:
VDS (DOVE)

Managing Office: Office of the Director/Volunteer Delivery System (VDS) Office

PIA Approval Date: 11/07/2024

PIA Expiration Date: 11/30/2027

1. **Is this a new or revised electronic information system? If revised, describe revisions.**

Revised – This is a three-year update to the PIA. DOVE was originally deployed using the vendor Kenexa in 2011. The technology was then acquired by International Business Machines (IBM) Talent Suite, and most recently acquired by Infinite Computer Solutions (ICS) Infinite Talent

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

X__ Both members of the public and Peace Corps personnel

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

The Peace Corps Act of 1961, as amended, 22 U.S.C. § 34. 2504(a)

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

The primary purpose of DOVE is to manage the application, pre-screening, and onboarding system for applicants, invitees, Peace Corps Volunteer (PCV)s and Peace Corps Response (PCR) Volunteers. The system contains data that is comprised of the individual’s application for volunteer service, the staff’s evaluation of the application and invitation to interview; detailed interview notes; the staff’s evaluation of the interview for suitability to determine if the applicant should be issued an invitation to serve as a Volunteer; additional evaluation, and placement. DOVE provides electronic service delivery and facilitates the exchange of Volunteer information from DOVE to the pre-service medical system, Medical Applicant Exchange (MAXx), using Microsoft Biztalk. It also shares information with the Peace

Corps Volunteer Database Management System (PCVDBMS) necessary to support the creation of Volunteer's profile as an Invitee and Trainee in IT systems Volunteer Information Lifecycle Application (VIDA) and the Chief Financial Officer's financial system, Odyssey. DOVE information is shared with the Travel Office via email so that the Travel Office can coordinate with the Department of State on an invitee's Passport and country Visa. DOVE streamlines business processes and effectively matches qualified applicants with meaningful assignments in the field as PCVs and PCR Volunteers.

DOVE is a commercial off the shelf (COTS) product hosted by Infinite Computer Solutions (ICS). It is comprised of two components for the application process: Infinite Talent BrassRing and Infinite Talent Onboarding. Individual members of the public first submit applications for PCV service and/or PCR service via the Applicant Portal (BrassRing). The VRS staff and PCR staff review and process the applications in BrassRing. Staff members then determine who is suitable to move forward as an invitee. Once an applicant becomes an invitee, the individual is asked to complete certain medical screening, training, and other requirements prior to placement and departure to their assigned post. Select staff have access to Onboarding to manage the candidate's onboarding data. Staff members can add key documents and information pertaining to the PCV or PCR's early termination at a later date. Onboarding is one of the two components of DOVE mentioned in the previous paragraph. All staff users have access to BrassRing, but a limited number have access to Onboard. They are two systems contained within the same online suite of products.

There is an additional workflow used for the Virtual Service Pilot (VSP) that is not available to any staff except those engaged with VSP. The VSP workflow is contained in DOVE. Unlike the PCV and PCR workflows, VSP data does not integrate with any other Peace Corps IT systems.

It allows VSP staff to collect Expressions of Interest (EOIs) from members of the public via an online portal and VSP staff can process the participants through the signing of the donation agreement. User type privileges in DOVE allow DOVE users to see only the information and candidates that they are allowed to see, and at appropriate stages of the application process.

5. List all forms of Personally Identifiable Information (PII) that is collected, maintained, or disseminated. The personal information is collected directly from the applicant who is a member of the public, and the PCV or PCR Volunteer and includes: Name, address, date of birth, telephone numbers, social security number, email address, race, sex or gender, national origin, ethnicity, marital status, dependent(s) name and date of birth (if applicable), education, financial obligations, legal history, drug and alcohol information, volunteer history, employment experience, military obligations, personal essay, foreign language skills; reference contact information such as first and last name, work title and/or work location, email address, and location; assignment and regional preferences, and other information relevant to the Volunteer positions that the Peace Corps provides to overseas Posts. PII that is also maintained includes the assigned Candidate Reference Number (CRN) and the assigned Volunteer ID number. Staff members may upload records associated with a Volunteer's early termination of service that includes: Consideration of Administrative Separation Memorandum, the Volunteer response, if any; and the Administrative Separation Memorandum.

DOVE disseminates the invitee's first, middle, and last name (full name), assigned CRN, home of record address, email, and phone number to the Travel Office to coordinate with the State Department to obtain a Volunteer's passports and Visas. DOVE also disseminates the successful candidate's full name, assigned CRN, and other pertinent details to the MAXx system. DOVE disseminates the following PII to PCVDBMS and Odyssey to create a volunteer profile: invitee's full name, date of birth, Social Security number, assigned CRN, home of record address, email address, phone number, gender, race, ethnicity, and spouse's name (if any).

The Virtual Service Pilot Participants submit similar PII in DOVE, but their data does not integrate with any additional systems internal or external to Peace Corps.

6. Why is PII being collected (e.g., to determine eligibility)? Does the IT system collects PII directly from individuals, or from another system? This information is being collected in order to assess the eligibility of PCV and PCR applicants for Peace Corps service, as well as to assess an applicant's technical competitiveness in relation to that of other applicants. This information is also being collected to assess the suitability of PCV and PCR applicants, including their Cultural Sensitivity, Emotional Maturity, Motivation and Commitment, and Productive Competence (technical skills). It is necessary to collect the applicant's Social Security number and birthdate because those two pieces of information allow the Peace Corps to confirm an applicant's identity, verify whether an applicant has ever applied and/or served before, and they are used as candidate (invitee) validation points in integrations with other Peace Corps systems. Information is collected directly from the individual, as well from other Peace Corps systems and Offices. The invitee's information will be shared with other Peace Corps systems to include MAXx, PCVDBMS, VIDA, and Odyssey, as well as information shared with the Travel Office for country visa requirements. In turn, MAXx and VIDA provide information that is either automatically populated with the applicant's personal information, or DOVE staff members can add to the individual's profile using keystrokes or upload documents.

For VSP, the data is collected directly from the interested individual to assess the eligibility of the interested participants in donating their time to the Virtual Service Pilot. It is not shared with any other systems.

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.

Yes, this information is shared with a system outside of the agency. From DOVE for all invitees, Travel and Transportation obtains the invitee’s full name, date of birth, country of service, and dates of service. This information is transmitted to the Special Issuance Agency, for the purposes of issuing their passports. The “Special Issuance Agency” is a separate entity within the Department of State.

The Travel and Transportation Office may obtain from DOVE for a handful of invitees, the invitee’s last name, date of birth, and last four digits of their social security number. This information is use through the Department of State’s online application status tracker U.S. Passport Application Status (state.gov), which is solely where the current processing status of applications is obtained from previously submitted via mail. No application data is entered into this online form.

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

Not applicable.

8. Notice of the collection of information.

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

X__ 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.

Each form listed in answer 8c has a Privacy Act Statement stating the Peace Corps’ legal authority to collect information from the individual, the purpose of collecting this information, the routine uses under the Privacy Act of 1974 and the Peace Corps, and notifies the applicant that disclosure of their online application and other forms is voluntary; however, failure to complete the forms will result in the Peace Corps inability to assess qualifications and suitability, and will preclude their consideration for volunteer service.

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.

Peace Corps Application, PC-1502
Peace Corps Response Application, PC-2119
Peace Corps Expedited Application, PC-1503
Peace Corps Response Expedited Application, PC-2192
Background Investigation Certification, PC-0005

Interview Rating Tool, PC-2134
Peace Corps Response Interview Assessment Form, PC-2135
Onboarding, PC-2174
Confidential Reference Form, PC-1532
Peace Corps Response Reference Forms, PC-2136, PC-2137, and PC-2138
Virtual Service Pilot Expression of Interest, PC-2196

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

Peace Corps Application, OMB Control Number 0420-0005
Peace Corps Response Application, OMB Control Number 0420-0547
Peace Corps Expedited Application, OMB Control Number 0420-0571
Peace Corps Response Expedited Application, OMB Control Number 0420-0572
Background Investigation Certification, OMB Control Number 0420-0001
Interview Rating Tool, OMB Control Number 0420-0555
Peace Corps Response Interview Assessment Form, OMB Control Number 0420-0556
Onboarding, OMB Control Number 0420-0563
Confidential Reference Form, OMB Control Number 0420-0006
Peace Corps Response Confidential Reference Form, OMB Control Number 0420-0548

Virtual Service Pilot Expression of Interest, OMB Control Number 0420-0547

9. Security.
a. What administrative, technical, and physical security safeguards/controls are in place to protect the PII? Every IT system has certain privacy risks. The administrative and technical privacy risks include unauthorized access, unauthorized disclosure, and a risk that the individual who added PII as an applicant provided erroneous information or writes down the user ID and password for a third person to gain access to that specific user account. There is also the risk that the wrong record will be uploaded to an individual's profile associated with close of service. There are administrative, physical security, and technical safeguards in place to mitigate these risks.

Administrative Controls: Only authorized Peace Corps personnel have restricted access to the system and its information based on a need-to-know basis to fulfill official duties and the need for certain roles. A Peace Corps staff member must submit an access request to the system administrator. Approval and access to DOVE's records is restricted to authorized Peace Corps personnel or federal contractors whose responsibilities require access. The senior DOVE administrator approves requests for access and assigns user roles to personnel who have an official need to know to perform their duties within the system. All authorized users are required to take annual Privacy Act training for the proper handling of personally identifiable information and their official responsibilities under the Privacy Act, and to sign the Peace Corps technical governance rules of behavior. Once an individual becomes a PCV invitee, the DOVE system will automatically send to them an email to access their own profile using a unique username and password. The invitee cannot access other invitees' profiles, nor access or change others' information. Authorized members of the ICS team, as the vendor, has access to the data in the capacity as the administrator and service provider for the system.

Physical Controls: The appropriate safeguards are in place for Headquarters. The vendor reports on its SOC 2 report that its server location in Sterling, Virginia meets physical security requirements.

Technical Controls: As a COTS product, DOVE has appropriate technical safeguards in place to include security access controls, boundary controls, detection, real time and historical audit logs to monitor system activity, user account authentication mechanisms to access and secure the information, appropriate firewalls, end to end encrypted data in transit and appropriately encrypted data at rest. Internal authorized PC staff can only access DOVE as privileged account holders from behind the PC firewall and must have an active directory account to log into DOVE. External authorized customers accessing DOVE must enter via the perimeter firewall and authenticate with the appropriate credentials. Management access is via a Virtual Private Network (VPN). Remote access to DOVE is encrypted to ensure confidentiality and integrity of information by a Transport Layer Security (TLS) Virtual Private Network

b. Has a system security plan been completed for the information system?
Yes, on 09/12/2024.

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-17 Peace Corps Volunteer Database Management System, and PC-21 Peace Corps Response Database.

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. Records in DOVE are scheduled as listed in Manual Section 892, Attachment A:

1. Input / Source Records (Disposition Authority: DAA-GRS-2022-0009-0002) [GRS 5.2, item 020]. Disposition: Temporary. Destroy upon verification of successful creation or update of the final record.

2. Master file records:
    a. DOVE Volunteer Recruitment and Applicant Records (Disposition Authority: DAA-0490-2016-0006-0001). Disposition: Temporary. Cut off at the end of the

fiscal year in which the final action is taken on the application. Destroy 6 years after cutoff.

b. Virtual Volunteer Recruitment and Application Records (Disposition Authority: DAA-GRS-2018-0008-0003) [GRS 2.1, item 180]. Disposition: Temporary. Destroy when 1 year old, but longer retention is authorized if required for business use.

   And

   Virtual Volunteer Recruitment and Application Records (Disposition Authority: DAA-GRS-2017-0007-0016) [GRS 2.2, item 110]. Disposition: Temporary. Cut off at end of year in which volunteer leaves. Destroy 4 years after cutoff but longer retention is authorized if required for business use.

c. DOVE Administrative Separation Records or "Resignation in Lieu of" Records: (Disposition Authority: DAA-0490-2016-0006-0003). Disposition: Temporary. Cut off at the end of the fiscal year in which the Volunteer is separated or resigns. Destroy 30 years after cutoff.

d. Requests for Trainees (Disposition Authority: DAA-0490-2016-0006-0004). Disposition: Temporary. Cut off at the end of the fiscal year. Destroy 3 years after cutoff.

3. Outputs (Intermediary Records – draft reports, data extracts, etc.) (Disposition Authority: DAA-GRS-2022-0009-0002) [GRS 5.2, item 020]. Disposition: Temporary. Destroy upon creation or update of the final record (report), or when no longer needed for business use, whichever is later.