PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: HireVue "Coordinate"

Managing Office: Office of Chief Information Officer (OCIO)

Privacy Impact Assessment (PIA) Approval date: June 20, 2023

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

HireVue's "Coordinate" tool is a revised system for the Peace Corps. Peace Corps is not using the HireVue "Live" tool mentioned in the PTA produced in 2020.

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.

22 USC 2504(a)- Peace Corps Volunteers, and 22 CFR Part 305- Eligibility and Standards for Peace Corps Volunteer Service

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

"Coordinate," HireVue's Software-as-a-Service (SaaS) tool, assists with the interview scheduling process for the Office of Volunteer Recruitment (VRS) and Peace Corps Response (PCR) staff. Coordinate will assist VRS and PCR with the scheduling of interviews with the general public and Peace Corps applicants. Coordinate allows the public to view a Peace Corps staff member's availability for interviews and self-schedule an interview at an available time.

HireVue is a FedRAMP-certified SaaS provider. The Peace Corps' Chief Information Officer (CIO) signed an Authority to Operate (ATO) with them in March, 2019. There is no facial recognition or artificial intelligence (AI) functionality associated with Coordinate. No audio or video recording will take place.

5. List all forms of Personally Identifiable Information (PII) that is collected, maintained, or disseminated. *Examples include first name, middle name or initial, last name, alternate names, birth date, place of birth, Social Security Number (full or partial), personal telephone number, personal address, personal email address, residency during service or host family address, family member information or third person contacts, driver's license number, passport number, Peace Corps Volunteer number, other ID number, gender/gender preference, race or ethnicity, religious preference, marital status, military service status or military records, legal, security, or law enforcement information or status, disability information or status, financial information, educational information, IEP address, MAC address, biometrics, photograph, electronic Protected Health Information.*

Peace Corps Staff:
Information will be maintained on Peace Corps **staff** members who have HireVue accounts for the sake of account creation. Staff member information collected/maintained for account privileges includes first name, last name, and work e-mail address. Office phone number is optional.

Leads:
Information from those who are seeking to apply to become applicants (**leads**) will be collected and maintained for the sake of account creation. Lead information collected and maintained includes first name, last name, and personal e-mail address. Leads can provide their cell phone number if they elect to receive text reminders.

Candidates:
Information from **candidates** who have applied to Peace Corps or Peace Corps Response includes first name, last name, and personal e-mail address. Candidates can provide their cell phone number if they elect to receive text reminders.

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 PII is collected for the sole purpose of creating an account with HireVue. HireVue collects PII directly from the public if the public accesses a staff person's calendar URL. PII may also be entered into HireVue by VRS or PCR in order to allow existing Peace Corps candidates the ability to self-schedule time to speak with them.

Staff PII will be manually entered by the OCIO System Administrator for HireVue when staff accounts are created. No PII belonging to staff is collected from another system.

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.

PII from HireVue will not be shared with another agency.

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?

☑ 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.

Without entering their first name, last name and e-mail address, members of the public cannot access HireVue in order to self-schedule time to speak with a Peace Corps or Peace Corps Response staff member. HireVue correspondence is not configurable to allow the PAS within the system; however, the corresponding emails to the public from Database of Volunteer Experience informing them to self-schedule their interview include a PAS.

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.

PC-2038.

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

OMB 0420-0005

9. Security.

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

Physical Controls: The privacy risks associated with this IT system are unauthorized access and unauthorized disclosure of PII. There are administrative, technical, and physical security controls in place to mitigate these risks. The physical controls are not outlined in this public document. A full description of the administrative, technical, and physical security safeguards/controls can be found in the HireVue GovCloud SSP.

Administrative Controls: HireVue access is granted to specific employees in VRS and PCR based on need-to-know role permissions. Staff with HireVue access requires users pass the agency security background checks, and any other hiring requirements deemed necessary by the Peace Corps for the creation of an Active Directory account with the Peace Corps. HireVue administrators can only grant a user access on an individual basis, which is limited by that user/staff member's specific role in the IT system. All staff take annual Privacy and cybersecurity training.

Technical Controls: The HireVue application is a FedRAMP-authorized SaaS solution. The HireVue information system is hosted within the Amazon Web Services (AWS) GovCloud infrastructure, which is also FedRAMP-authorized. Data is encrypted in transit and at rest. Within the HireVue GovCloud production system, HireVue protects customer data at rest and provide customer data isolation within all databases. The data is encrypted with a custom encryption key from AWS Key Management Service (KMS), which creates a key and uses

encryption to protect the data. KMS uses AES-256 symmetric keys and is FIPS validated (certificate#3139). HireVue data and logs are backed up to the AWS S3 service. S3 buckets are automatically encrypted by AWS with AES-256 encryption.

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

Yes. The most recent system security plan (SSP) is dated January 19, 2023. The Peace Corps has had an ongoing authority to operate (ATO) since March 12, 2019.

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.

This IT system is covered by the agency System of Records PC-17, Peace Corps Volunteer Database Management System as it pertains to the application process. Names and e-mail addresses of Peace Corps staff are covered under the "Rolodex Exception" and do not require a SORN.

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-2014-0002-0008 [GRS 2.1, item 090]. Retention: Destroy records two years after case is closed by hire or non-selection.

This Privacy Impact Assessment has been evaluated by the following officials:

Systems Manager (submitter):

_____ Date: _____
(Signature)

Name, Title: _____

Authorizing Official (CIO):

_____ Date: _____
(Signature)

Name, Title: _____

Agency Records Officer

_____ Date: _____
(Signature)

Name, Title: _____

Reviewing Official (OGC):

_____ Date: _____
(Signature)

Name, Title: _____

Privacy Act Officer (final clearance):

_____ Date: _____
(Signature)

Name, Title: _____

Detach this signed coordination page prior to public release.

DIRECTIONS

Complete the Peace Corps Privacy Impact Assessment (PIA) for an electronic information system or electronic collection that contains Personally Identifiable Information (PII). The purpose of this form is to evaluate privacy and security controls of an IT system and to document the risk assessments of an IT system maintaining PII. Conduct a PIA before an office creates a new system collection or procures information technology. Use the PIA to identify how the electronic system collects, maintains, uses, and disseminates PII, possible risks, safeguards to against such risks, and how the agency manages the lifecycle of those records.

The prescribing authority for this form is the E-Government Act of 2002, Section 208 (b) (Pub.L. 107-347, 44 U.S.C. § 101), OMB Memorandum M-03-22, Appendix A, and OMB Circular A-130. The office component responsible for this form is the Privacy Act Office.

1. Fill out this form using Arial font, size 11.
2. Commence a PIA before your office develops a new electronic collection, or before you significantly modify an existing IT system or information collection.
3. The IT System Manager is responsible for completing the PIA and support meetings.
4. Email the final PIA draft to the Privacy Act Officer for approval prior to routing for signature.
5. The FOIA Officer will provide the System Manager with a fillable PDF for digital signature.
6. Digitally sign on the coordination page with PIV card credentials.
7. Electronically route the remaining coordinating signatures.
8. Submit the electronically signed document to the FOIA/Privacy Officer for signature.
9. The Privacy Act office will post the completed PIA online through the webmaster. The Coordination page will be removed prior to public posting.
10. Contact the Privacy Act Office at PrivacyOffice@peacecorps.gov for assistance.

Guidance for System Manager:

The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.

1. **IT development stage**. PIAs conducted at this stage will:
   a. Address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
   b. Address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in the attached questions, to the extent these elements are known at the initial stages of development;
   c. Need to be updated before deploying the system to identify elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.

2. **Major information systems.** PIAs conducted for these systems should reflect more extensive analyses of:
   a. the consequences of collection and flow of information,
   b. the alternatives to collection and handling as designed,
   c. the appropriate measures to mitigate risks identified for each alternative and,
   d. the rationale for the final design choice or business process.

3. I**nformation life cycle analysis/collaboration**. Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. The PIA require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.