PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Microsoft SharePoint (SP)

Managing Office: Office of the Chief Information Officer

PIA approval date: 10/04/2021

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

This is a new Privacy Impact Assessment for an existing IT system.

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

X 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 of 1961, 22 U.S.C. § 2503; the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551; Executive Order 14043, *Requiring Coronavirus Disease 2019 Vaccination for Federal Employees,* (Sept. 9, 2021); Executive Order 13991, *Protecting the Federal Workforce and Requiring Mask-Wearing* (Jan. 20, 2021), Executive Order 12196, *Occupational Safety and Health Program for Federal Employees* (Feb. 26, 1980), and 5 U.S.C. chapters 11, and 79.

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

The Peace Corps' Microsoft SharePoint environment enables collaboration and information sharing throughout the agency. It is used to distribute official federal and agency guidance to Peace Corps personnel, and houses library repositories, and collaborative pages to manage, inform, and track key documents, data and program requirements. Individuals can also directly add information into intake forms, spreadsheets, or upload documents to a designated data collection repository that may be restricted to privileged users. Our SharePoint environment is part of the Peace Corps General Support System (GSS). Peace Corps is collecting Personal Health Information (PHI) -- the COVID-19 vaccination status of its employees and contractors -- pursuant to the listed Executive Orders, the Safer Federal Workforce Task Force COVID-19 Workplace Safety: Agency Model Safety Principles (July 29, 2021), and the

Task Force's Frequently Asked Questions on Vaccinations (August 6, 2021). To support this effort, Peace Corps' employees and contractors will provide information regarding their COVID-19 vaccination status to authorized staff in the Office of Safety and Security through a link to Peace Corps' secure SharePoint platform. Other than authorized system administrators, only authorized members of the Privacy Office, and those who have responsibilities related to a project have a need to know, will have access to employee and contractor responses.

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.*

PII may include the following, depending on the specific purpose of the uploaded record or the official collection determined by an Office or Working Group: First name, middle name, last name, personal email address, personal phone number, work email address, work phone number, job our duty position, assigned office, assigned supervisor, Country of duty station, Post duty station, PHI, PII associated with federal compliance, gender or preferred gender, disability information or status, photograph or facial image, travel and financial information.

6. Why is PII and PHI being collected (e.g., to determine eligibility)? Does the IT system collects PII directly from individuals, or from another system?
PII and its subset, PHI, are collected both directly from the individual and indirectly to complete specific program objectives and requirements, based on the office or working group responsible for the specific SharePoint page or based on the uploaded file to that page.

7. Sharing and Disclosure.

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

No information from SharePoint will be directly shared system-to-system with another agency. Some information may be shared by the agency as a general routine use under the Privacy Act of 1974, or under the agency's routine uses, or a specific routine use in accordance to a System of Records Notice.

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 _X_ Both

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.

The person has the opportunity to object if the individual is directly asked for information on that page, form, or spreadsheet unless that form is mandatory in the federal government. A person does not have the opportunity to object if this record is uploaded from official office files for internal business purposes.

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

See the official Peace Corps Forms Library Intranet page in SharePoint.

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

Not applicable. This does not collect information from the public.

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 associated with this system include unauthorized access; unauthorized disclosure of PII, to include PHI; and a risk that the individual who adds PII may provide erroneous information or upload the wrong record. Peace Corps has administrative, technical, and physical security controls in place to mitigate these risks.

Administrative controls: All Peace Corps personnel are required to successfully complete both the annual IT security training and the annual Privacy Act training, and sign the Peace Corps technical governance rules of behavior. Individuals with approved intranet access and the appropriate Personal Identity Verification credentials can visit the Peace Corps SharePoint platform. Only authorized Peace Corps personnel have access to restricted SharePoint pages and content, or audit logs based on a need-to-know basis to fulfill official duties or delegated roles. A Peace Corps staff member or contractor must submit an access request to the page/site owner to gain access to restricted content. Approval and access to a particular site/page is restricted to authorized Peace Corps personnel or federal contractors whose responsibilities require access, and is approved by the individual(s) in the office managing that page or library. Authorized members of the Office of the Chief Information Officer have access to the data in the capacity as the administrator for SharePoint, or that particular page or library.

Physical controls: The appropriate safeguards are in place for Headquarters, and for the data center colocation in Ashburn, Virginia.

Technical controls: SharePoint technical safeguards and controls pertain to the GSS boundary in which it resides. The technical controls in place include firewalls, system access, encrypted data at rest, and encrypted data in motion. SharePoint access is restricted to Peace Corps individuals who have intranet access through Personally Identity Verification or assigned RSA token for general login access. Privileged users access and authenticate via single sign on from the Peace Corps Active Directory. Audit logs allow for the privileged user or administrator to review for unusual activity. Extensive Federal Information Security Management Act (FISMA) and NIST SP 800-53 controls are in place. Requirements defined in OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016) are in place to secure the data at rest and in transit. The Peace Corps secures encrypted data in transit by transferring it via Transport Layer Security. Federal Information Processing Standards (FIPS) 140-2 are enabled on all MS Windows OS server. SharePoint Servers use encryption for computing hash values that do not comply with FIPS 140-2, Security Requirements for Cryptographic Modules. These algorithms are not used for security purposes; they are used for internal processing. For example, Peace Corps SharePoint Server uses MD5 to create hash values that are used as unique identifiers. Since SharePoint Server uses these algorithms, it does not support the Windows security policy setting that requires FIPS compliant algorithms for encryption and hashing. This Windows security policy is managed through the FIPSAlgorithmPolicy registry key in Windows. Storage level encryption are implemented on SQL and SharePoint Servers.

b. Has a system security plan been completed for the information system?
Yes. SharePoint is a component of the PCGSS information system, which had its last system security plan published on June 24, 2021.

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

All agency SORNs may be applicable, depending on the Office that manages the particular record collection within the platform. Specifically:

GSA/GOVT-7, HSPD–12 USAccess (Federal Personal Identity Verification Identity Management System (PIV IDMS))

OPM/GOVT-1, General Personnel Records
OPM/GOVT-10, Employee Medical File System Records
PC-3 – Contractors and Consultants Files
PC-11 – Personal Services Contracts
PC-17 – Peace Corps, Volunteer Applicant and Service Records System
PC-26 – Peace Corps Computer Systems Activity and Access 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.

The information collected is subject to the NARA GRS or a NARA-approved disposition schedule. Users must refer to Manual Section 892, Attachment A for the specific record disposition instructions under the Office responsible for that record created/saved on this system. Treat any unscheduled records as permanent, and consult the Agency Records Officer.