PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Peace Corps Security Operations Center (PCSOC)

Managing Office: Office of the Chief Information Officer (OCIO)

PIA Approval Date: October 4, 2024

PIA Expiration Date: October 31, 2027

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

This is an updated electronic information system.

As part of the social engineering testing, Peace Corps has subscribed to a third party KnowBe4's Security Awareness Training and Simulated Phishing platform (KMSAT) to manage IT security problems of social engineering, spear-phishing, and ransomware attacks. The Penetration Test Laptop has been added as a component to PCSOC system boundary to conduct penetration tests for Peace Corps systems.

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.

22 U.S.C § 34. 2501(a) et seq., The Peace Corps Act of 1961, as amended; 40 USC11315, Agency Chief Information Officer; 44 USC 3506, the Paperwork Reduction Act, as amended by the Information Technology Management Reform Act of 1996, Section 5125(a) of Pub. L. 104-106 (Clinger-Cohen Act); 44 USC 3541 et seq., the Federal Information Security Management Act of 2014 (FISMA), Public Law 113-283; OMB Circular A-130, Management of Information Resources.

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

The SOC manages incidents for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event) and determine if it is a real, malicious threat (incident), and if it could have a business impact.

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

First Name, Middle Name or Initial, Last Name and Email Address

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

The information is being collected to enroll personnel with active Peace Corps email to the social engineering testing and training. Account creation for access to the system requires the first name, last name, middle initial, employee / contractor email address.

The PII is collected either through a manual process or direct connection to Peace Corps Global Support System (PCGSS).

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.

No, information will not be shared with another federal 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 (N/A)

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 _X_ 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.

The individual cannot consent because their information is automatically obtained from PCGSS for this system.

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.

N/A

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

N/A

9. Security.

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

Administrative Controls:
PCSOC follows the organizational policies with regards to personnel signing the Rules of Behavior (ROB) before being granted access to the Peace Corps systems/applications and data. All PCSOC employees also undergo an annual training and awareness training on data privacy laws, safe handling of PII, and the organization's policies regarding PII protection.
Access controls to PCSOC follows the principle of least privilege. All user access is provided according to the minimal access to perform job functions. PCSOC also conducts periodic review of user accounts to ensure only authorized personnel have access to PII and application. The PCSOC team also reviews audit logs and regularly monitors these logs for suspicious activities.

Technical Controls:
Access to the system requires multi-factor authentication. A user must be logged on to the Peace Corps network, having been provided access by IT Security after reading and signing Rules of Behavior by the individual.

Peace Corps utilizes TLS 1.2 to ensure data encryption in transit and the Network attached storage of the PC-GSS is encrypted with a FIPS 140-2 validated crypto module. The encryption algorithm used is an NSA approved encryption algorithm utilizing a 256-bit key.

Data communication between the web customers and KnowBe4's backend systems are encrypted using SSL/TLS which protects data in transit. Data is held in an encrypted Amazon Relational Database Service (RDS), which provides for availability and data durability. Storage is provided by encrypted Amazon Simple Storage Service (S3) buckets dedicated to KnowBe4. Encryption is enabled to protect data at rest.

Physical Control: The appropriate physical controls for both Peace Corps and Vendor locations meet physical security requirements.

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

Yes. The system security plan was completed on August 20, 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.

Names and e-mail addresses of Peace Corps staff are covered under the "Rolodex Exception." The system will contain the names, work addresses, work email addresses, and work phone number of agency personnel and contractors working for the Peace Corps. The context for use of this information will be to contact the individual for routine business matters.

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-18, Former Peace Corps Volunteer and Staff Database.

PC-26, Peace Corps Computer Systems Activity and Access Records.

PC-36, Personnel Accountability System.

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 records related to the PCSOC product/services outlined above are covered by the following disposition authorities:

DAA-GRS-2013-0005-0010 / 040 Information Technology Oversight and Compliance Records.
Information Technology (IT) Oversight and Compliance records relate to compliance with IT policies, directives,
and plans. Records are typically found in offices with agency-wide or bureau-wide responsibility for managing IT
operations. Includes records such as:
• recurring and special reports
• responses to findings and recommendations
• reports of follow-up activities
• statistical performance data
• metrics
• inventory of web activity
• web use statistics
• comments/feedback from web site or application users

• internal and external reporting for compliance requirements relating to the Privacy Act, and electronic and information technology accessibility under Section 508 of the Rehabilitation Act
• system availability reports
• target IT architecture reports
• systems development lifecycle handbooks
• computer network assessments and follow-up documentation
• vulnerability assessment reports
• assessment and authorization of equipment
• Independent Verification and Validation (IV&V) reports
• contractor evaluation reports
• quality assurance reviews and reports
• market analyses and performance surveys
• benefit-cost analyses
• make vs. buy analysis
• reports on implementation of plans
• compliance reviews
• data measuring or estimating impact and compliance

Disposition: Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded.

And

DAA-GRS-2013-0006-0001 / 010 Systems and Data Security Records
These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Includes records such as:

• System Security Plans
• Disaster Recovery Plans
• Continuity of Operations Plans
• published computer technical manuals and guides
• examples and references used to produce guidelines covering security issues related to specific systems and equipment
• records on disaster exercises and resulting evaluations
• network vulnerability assessments
• risk surveys
• service test plans
• test files and data

Disposition: Temporary. Destroy 1 year after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.