PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Cyber Security Assessment and Management (CSAM)

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

PIA Approval date: March 3, 2023

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

This is not a new electronic system; however, this is the first PIA for this 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 (22 U.S.C. 2501 et seq.), as amended; The Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. Sections 3551 – 3558; OMB Memorandum, “Security Authorization of Information Systems in Cloud Computing Environments,” December 8, 2011; Revision of OMB Circular A-130, “Managing Information as Strategic Resource.”

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

The CSAM application supports Certification and Accreditation activities at Peace Corps for FISMA Reporting. CSAM provides the Peace Corps a web-based secure network capability to assess, document, manage and report on the status of IT security risk assessments and implementation of Federal and agency-mandated IT security control standards and policies. CSAM is critical to both security personnel and IT security program managers. Security control assessors rely on the delivery of timely, detailed

information and policy tool support related to IT Standards implementations. The use of the CSAM application enables system owners and security managers to obtain system performance information from a multitude of security related processes, while enabling the Peace Corps to meet mandated enterprise and system reporting requirements.

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.*)

The system collects PII that includes: the employees/federal contractors/Peace Corps Volunteers' full name, office address, office telephone number, official work email, and staff ID of individual federal staff members and federal contractors who maintain official roles and responsibilities where applicable.

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

Employee and contractor name, organization, title and official contact information are collected and used in CSAM to support the Peace Corps information assurance programs to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight.

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, data may be shared with the Office of Management and Budget under OMB Circular A-123.

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

Interconnection Security Agreement (ISA); Service Level Agreement (SLA)

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.

Users are presented with Privacy Notice warning banner that informs them they are accessing a Peace Corps system, that they are subject to being monitored, and there is no expectation of privacy during use of the 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.

Not applicable (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 include ensuring that only authorized personnel have restricted access to the designated system based on a need-to-know basis to fulfill official duties. System administrators within the OCIO assign user roles to limit access to only those who have an official need to know to fulfill their responsibilities. Authorized users are trained in the proper handling of PII and in their official duties under the Privacy Act and the Peace Corps technical governance for the rules of behavior. Contractors supporting information assurance functions are subject to all the same requirements as federal employees.

Technical safeguards include the use of access controls and user account authentication mechanisms to secure information, as well as the use of audit logs. Computer access requires a Personal Identity Verification (PIV) badge and appropriate credentials for user authentication.

Physical controls include security guards within the facility; PIV badge access is required for entrance into the building; and security cameras are in place.

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

Yes, a System Security Plan was signed by the Authorizing Official, System Owner and Information Systems Security Officer on 1/13/2023.

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-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.

General Technology Management Records

Systems and Data Security Records, disposition authority DAA-GRS-2013-0006-0001 [GRS 3.2, item 010]. Record 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.

GRS 3.1, item 040 Information technology oversight and compliance records DAA-GRS2013-0005-0010. Record disposition: Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.