PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: CrowdStrike

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

PIA Approval Date: August 22, 2024

PIA Expiration Date: August 31, 2027

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

New System

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; Federal Information Security Modernization Act of 2014, as amended (FISMA); E.O. 14028, Improving the Nation's Cybersecurity (May 12, 2021; National Institute of Standards and Technology (NIST) cybersecurity framework; SP 800-221- Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio (Nov 17, 2023);Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (February 12, 2013).

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

This IT system is a cloud based FedRAMP Moderate Software as a Service (SaaS) solution offered as part of the CDM DEFEND F Asset Management (AM) Shared Services Catalog product suite to provide Next-Generation Anti-Virus (NGAV) capabilities that supports the Peace Corps Security Operations Center (PCSOC) program to manage cyber incidents for the enterprise, ensuring they are properly

identified, analyzed, communicated, actioned/defended, investigated and reported. The CDM CrowdStrike Falcon offering supports the CDM Dashboard and provides Peace Corps a robust toolset to increase endpoint security posture in the PC environment. CrowdStrike Falcon Complete provides the Peace Corps 24/7 managed detection and response (MDR) for Virtual infrastructure, Servers, Windows and Apple endpoints. CrowdStrike provides Peace Corps with improved capabilities for early detection, response, and remediation of cybersecurity incidents on PC network, using advanced technologies and leading practices.

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

PII appearing in machine event fields, such as the first name, last name, middle initial, usernames, machine names, email addresses of Peace Corps employees/contractors and IP addresses.

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

Account creation for access to the system requires the first name, last name, middle initial, employee / contractor email address and username information. Machine event data is monitored to detect, prevent, and respond to cybersecurity attacks. Machine event data may include user account, computer name, host name, and other system identities as well as file names and files paths. Therefore, PII may be collected to the extent that it exists in a collected field.

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. As part of the user account creation process, the first name, last name, middle initial, employee / contractor email address and User ID information is shared with the Cybersecurity and Infrastructure Security Agency (CISA). CISA manages the Shared Services Catalog Platform which Peace Corps is a tenant. Accounts cannot be created without providing the required user account data.

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

Yes. There is a Memorandum of Agreement between Peace Corps and Cybersecurity and Infrastructure Security Agency relating to the Continuous Diagnostics and Mitigation Capability Shared Service Platform.

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 system does not collect PII directly from individuals. Instead, the system process machine event data from Peace Corps Virtual infrastructure, Servers, Windows and Apple endpoints which may incidentally include PII.

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?

CrowdStrike agents do not collect document file contents but instead are narrowly tailored to focus on machine event data. The data is encrypted in transit to the cloud and at rest within the cloud. Access to the machine event data is strictly controlled by need to know, strong authentication, encrypted sessions and access logging as per FedRAMP requirements.

Based upon roles, specific CrowdStrike team members engaged in engineering, security, and threat analysis have access to the systems that may contain PII. These authorized personnel require access to the systems and services as administrators to ensure that the system is maintained appropriately.

Specific CrowdStrike Platform Security Operations team members will have authorized access to data generated by the systems within the Falcon Platform. They may view PII data as a result of reviewing log data generated by the platform when federal customers use the system.

There are administrative, technical, and physical security controls in place to mitigate risk associated with the use of the system.

Administrative (personnel) controls: Only designated authorized Peace Corps personnel who support the Office of the Chief Information Officer are granted access to PCSOC information. Designated personnel are assigned system access based on work-related duties and responsibilities. Certain authorized Peace Corps staff members and contractors are approved for access after taking initial privacy and security training (with recurring annual training), and then submitting a request for access. The vendor ensures the appropriate privacy and security training for its support staff. A designated privileged account user reviews the request submission to ensure the staff member meets the appropriate requirements for access. Access controls to PCSOC follows the principle of least privilege. User access is provided according to the minimal access required in order to perform job functions.

Technical Controls: Access to CrowdStrike requires multi-factor authentication.
Peace Corps utilizes TLS 1.2 to ensure data encryption in transit and the Network attached storage of the PCGSS is encrypted with a FIPS 140-2 validated crypto module.
The CrowdStrike Falcon Platform protects the confidentiality and integrity of transmitted information over untrusted networks through the implementation of cryptographic mechanisms for data in transit and data at rest. All data communications are encrypted using FIPS 140-2 validated crypto modules. Ciphers used within the Falcon Platform include:

- Web-based traffic is transmitted and encrypted using a minimum of TLS 1.2 and AES-128 ciphers.
- Administrative connections over SSH are protected using FIPS-validated ciphers and hashes.
- Email for custom alerts to customers, while not containing federal data, are encrypted using TLS encryption supported by the Amazon Simple Email Service (SES) on TCP port 587 which includes up to TLS 1.2 and AES-256.

Physical Controls: Appropriate physical controls are in place for Peace Corps. As per CrowdStrike SaaS approved FEDRAMP SSP, the vendor is maintaining physical and environmental protection mechanisms to protect PII.

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

No. The SSP is expected to be completed by 10/31/2024.

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.

No SORN exists at this time. A SORN will need to be created for this new 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.

DAA-GRS-2013-0006-0001 GRS 3.2 item 010 “Systems and data Security Records” Temporary. Destroy 1 year(s) 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. (02/27/2024)