PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Qualys

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

PIA Approval date: July 1, 2024

PIA Expiration date: July 31, 2027

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

New electronic information 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.), Federal Information Security Modernization Act of 2014, as amended (44 U.S.C. 3551-3558), U.S. Code of Federal Regulations (CFR) 5 Part 293.302, 5 CFR 293.303, 5 USC §§ 1104, 1302, 2951, 3301, 3372, 4118 4315, and 8347; 3 CFR 1954-1958 Comp.; 5 CFR 7.2; Executive Order (E.O.) 9397, as amended, *Numbering System for Federal Accounts Relating to Individual Persons* (*November 22, 1943)* as amended by E.O. 13478 (November 18, 2008); E.O. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 17, 2017); E.O. 14028, *Improving the Nation's Cybersecurity* (May 12, 2021); 3 CFR 1943-1948 Comp.; 5. 5 CFR Chapter 1 part 293 Personnel Records and Peace Corps 22 CFR 2501 et seq.; OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003); OMB Memorandum M-17-12: Preparing for and Responding to a Breach of Personally Identifiable

Information (January 3, 2017); OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems (November 18, 2013); OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices (October 3, 2014); and OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (October 30, 2015), OMB Circular M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (August 27, 2021).

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

Qualys consolidates and evaluates vulnerability data across Peace Corps, prioritizing security risks and providing a clear view of your security posture. The solutions enable Peace Corps to identify security risks to Peace Corps IT infrastructure, help protect IT systems and applications from cyber-attacks and achieve compliance with internal policies and external regulations. The Qualys Cloud Platform (QCP) offering consists of an integrated suite of solutions, including Vulnerability Management, Web Application Scanning and Policy Compliance. The QCP assist the Peace Corps to:

• Define policies to establish a secure IT infrastructure in accordance with good governance and best practices frameworks.

• Discover and catalog all assets, no matter where they reside, inside the enterprise, on the perimeter, or in the cloud.

• Automate ongoing security assessments for IT systems and web applications.

• Mitigate risk and eliminate threats

• Monitor and measure network compliance in one unified console—saving time, assuring reliability, and reducing costs.

• Distribute security and compliance reports customized to meet the unique needs of business executives, auditors, and security professionals.

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 includes: First name, last name, middle initial, employee / contractor email address and User ID information.

6. Why is PII being collected (e.g., to determine eligibility)? Does the IT system collect 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 User ID information.

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 scans Peace Corps Virtual infrastructure, Servers, Windows and Apple endpoints for vulnerabilities which may incidentally include PII. The system also requires Peace Corps employees and contractors' first name, last name, middle initial, email address and User ID information as part of the account creation process.

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?

The administrative, technical, and physical privacy risks include unauthorized access and unauthorized disclosure. There are administrative, physical security, and technical safeguards in place to mitigate these risks. A full description of the administrative, technical, and physical security safeguards/controls can be found in the Qualys System Security Plan (SSP).

Administrative Controls: Qualys access is granted to specific employees in Peace Corps based on need-to-know and their role and permissions. Staff with Qualys 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. Qualys 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: Access controls and user account authentication mechanisms are used in securing the data. Computer access requires a Personal Identity Verification (PIV) Badge and appropriate credentials. The Qualys application is a FedRAMP-authorized SaaS solution. Qualys Cloud Based Security Software as a Service (SaaS) solution offered as part of the CDM DEFEND F Asset Management (AM) Shared Services Catalog product suite. Data is encrypted in transit and at rest. Within the Qualys Cloud Platform (QCP), Qualys protects customer data at rest and provides customer data isolation within all databases. Physical servers have local storage which is also encrypted with AES-256 bit. These servers are part of respective clusters: Cassandra and Kafka. Data is replicated across multiple server nodes; so, failure of one server/storage location is not critical. Backup is stored on OCI object storage on the gov cloud and encrypted with AES-256 bit.

Qualys' end-to-end data security architecture includes:

- All communication in HTTPS (TLS)
- Encrypted authentication credentials
- Encrypted vulnerability data
- Hardened appliances with no listening services or open ports
- Ongoing review of SOC controls

Physical Controls: The QCP production environment is physically and logically isolated from other Qualys IT systems and only select employees have physical and/or logical access to this infrastructure. Data centers are owned and operated by Cyxtera and Oracle Cloud Infrastructure respectively, and are physically hardened facilities, including the use of non-descript buildings, limited entrance ways, video surveillance, human guards, multi-factor authentication systems, and man traps, and are engineered to withstand a significant natural disaster.

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

No. The SSP is expected to be completed by 7/10/2024.

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 QUALYS 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.