PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Peace Corps General Azure Infrastructure (PCGAI)

Managing Office: Office of the Chief Information Officer

Privacy Impact Assessment (PIA) Approval date: April 19, 2024

1. Is this a new or revised electronic information system? If revised, describe revisions. Identify any contract vendors that host this system.

PC75 Peace Corps General Azure Infrastructure (PC75 PCGAI) is a new non-FISMA system. PC75 PCGAI is our Microsoft Azure Commercial Cloud that is a JAB FedRAMP Authorized (Package ID F1209051525) Cloud Service Offering (CSO):

System Profile

Service Model: IaaS, PaaS, SaaS
Deployment Model: Public Cloud
Impact Level: High

Business Use

PC75 PCGAI functions primarily as a disaster recovery (DR) environment to support fail-over, recovery, and restore activities to the Peace Corps General Support System (PC45 PCGSS) located in an Equinix Data Center (known as Peace Corps CoLo) in the event of a severe service disruption. The course of action would be to execute full data center fail-over of critical infrastructure and applications to the Microsoft Azure Commercial Cloud disaster recovery site for resumption of operational capabilities, perform recovery phase activities in the CoLo, to restore system capabilities affected by the service disruption, and restore the CoLo environment to resume normal operational capabilities.

The authorization boundary for PCGAI consists of the network, computer, storage, and security infrastructure hosted in the FedRAMP Authorized Microsoft Azure Commercial Cloud (Package ID F1209051525). Microsoft Azure interconnects with PC45 PCGSS located in the CoLo by way of two (2) Azure Express Route connections. Microsoft Azure Commercial Cloud is used for the following:

1) Essential Infrastructure: Required to operate and maintain the Microsoft Azure Commercial Cloud environment.

- Domain Controllers (Access Management)
- Azure Express Route: Provides connection between Microsoft Azure Commercial Cloud and the Equinix Data Center (CoLo)
- Tenable scanner (Security and Compliance)

2) Disaster Recovery (DR)

- CommVault: Storage Replication facilitates copying of the data to off-site data storage volumes in the Microsoft Azure Commercial Cloud DR environment. These storage volumes are designated as critical to the Agency.
- Virtual Machines (VM): These VMs are designated as critical to the Agency.
- CyberArk: Live backup for privileged access management in the event of a service disruption in the CoLo.
- Financial Databases: Live Backups.
- NetApp: Live Backup of File Shares.
- Palo Alto Firewall: Provides VPN access into the Azure DR site.

3. Volunteer access to Agency CRM via Microsoft Azure Commercial Cloud Web Application Proxy (WAP) and Web Application Firewall (WAF)

Description/Environment:

Location: Microsoft managed United States Data Centers. Infrastructure Services fully inherits the protection of power equipment and cabling from damage and destruction from the Microsoft Azure Commercial Cloud FedRAMP Authorization.

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; FIPS 200, Minimum Security Requirements for Federal Information and Information Systems; NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems; the Records Management Act of 1950, as amended, 44 U.S.C. 31; Executive Order 14028 – Improving the Nations Cybersecurity (May 12, 2021); OMB Circular A-130, Managing Information as a Strategic Resource; OMB Circular M-24-4, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements; NIST SP 800-82, rev.3 - Guide to Operational Technology (OT) Security; OMB Circular A-130, rev. 4, Managing Information as a Strategic Resource (2021); 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).

PC75 PCGAI functions primarily as a disaster recovery (DR) environment to support fail-over, recovery, and restore activities to the Peace Corps General Support System (PC45 PCGSS) in the event of a severe service disruption. The course of action would be to execute full data center fail-over of critical infrastructure and applications to the Microsoft Azure Commercial Cloud disaster recovery site for resumption of operational capabilities, perform recovery phase activities in the CoLo to restore system capabilities affected by the service disruption, and restore the CoLo environment to resume normal operational capabilities.

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

PCGAI platforms, messaging, and cloud services for supported applications may contain PII that is collected, maintained or disseminated, to 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, and electronic Protected Health 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?

PCGAI does not collect PII directly from individuals. PCGAI collects, maintains, and stores PII through its connections to the PCGSS in its function as a disaster recovery environment.

PCGAI functions primarily as a DR environment to support fail-over, recovery, and restore activities to the PC45 PCGSS. PCGSS is the Network Computer, back up and Network Storage infrastructure for the Peace Corps and does not collect PII directly. The authority to collect PII is documented in the System of Records Notice (SORN) and/or PIA documentation of the systems that directly collect PII. Any PII data that is collected, maintained, or stored in the PCGAI system would be the same PII data that is collected, maintained, and stored in the PCGSS environment that is replicated to the PCGAI DR environment.

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, the information the PCGAI collects will not be shared with another agency. If an individual system that sits on PCGAI decides to share information, it should be documented in the PIA of that system.

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 PCGAI does not directly collect PII because information is obtained from an existing information system or source. The PCGAI system is only the storage medium for Peace Corps systems. The PII that the system collects is to help managed Peace Corps employees, and contractors and to help the business operations of the agency.

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?

PCGAI is required to follow the NIST SP 800-37, Rev.2 Risk Management Framework for Information Systems and Organizations. PCGAI is continuously subjected to the

RMF Prepare, Categorize, Select, Implement, Assess, Monitor and Authorize tasks. In addition, PCGSS follows Manual Section 542, Information Security Program.

PCGAI will undergo an annual security assessment of administrative, technical, and operational security controls derived from NIST SP 800-53. Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations. Using the NIST SP 800-53 Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations, the authorized users will use the recommended methodology to examine, interview, and test its systems. Peace Corps selected moderate security controls are assessed by an independent third party to validate that the security controls are in place and operating as intended.

PCGAI is a FedRAMP Moderate Cloud Service Offerings (CSO). Infrastructure Services administrators and security personnel review FedRAMP security packages and configure, implement, and test customer responsible security controls prior to being granted an Authority to Use (ATU) / Authority to Operate (ATO) from the Authorizing Official (AO).

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

PCGAI has a current System Security Plan (SSP) with an expected approval date of May 3, 2024 that is reviewed and approved by the AO or designated representative prior to plan implementation. The PCGAI ISSO updates the SSP to address:

1. changes to the information system/environment of operation;
2. problems identified during plan implementation;
3. problems identified during security control assessments.

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.

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.

Provides platform for program offices. PCGAI will not directly modify or delete any records associated with programs in PCGAI. PC program offices are responsible for all records management requirements.

DAA-GRS-2013-0006-0005 – GRS 3.2/040 “System backups and tape library records - Incremental Backup Files” - Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

DISPOSITION: TEMPORARY. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

And

DAA-GRS-2013-0006-0006 – GRS 3.2/041 “System backups and tape library records – Full Backup Files” - - Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

DISPOSITION: TEMPORARY. Destroy when a second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.