Privacy Impact Assessment: Infrastructure Systems

SECTION V
PRIVACY QUESTIONS

Infrastructure Systems
Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Volunteer, Employee, Other.

Infrastructure systems include: desktops, laptops and the servers that support domestic and overseas operations. These systems contain operating system (O/S) software, firmware, and office support software. In addition, there are various applications and databases that are hosted in the infrastructure system which are maintained and managed by the application owners.

2. What are the sources of the information in the system?

The O/S and firmware are provided by the hardware vendors.

The various types of information and data hosted on infrastructure systems (e.g., databases. spreadsheets. memorandums, etc…) are entered by Peace Corps staff.

a. What Peace Corps files and databases are used?

At the O/S and firmware level no Peace Corps files or database are used.

All Peace Corps hosted applications/system files and databases on located on infrastructure equipment. For example files created with Microsoft Office software (e.g., Word, EXCEL, PowerPoint and Access) as well as other major databases and systems are stored on infrastructure equipment.

b. What Federal Agencies are providing data for use in the system(s)?

Nothing is provided at the O/S or firmware level.

For hosted applications/systems the USDA National Finance Center provides payroll updates and the State Department provides financial updates and software systems.

c. What State and Local Agencies are providing data for use in the system(s)

None

d. What other third party sources will data be collected from?
Software patches and operating system upgrades from software vendors.

e. What information will be collected from the volunteer/employee?
None for the O/S and firmware levels

For applications hosted on infrastructure equipment this information could include personnel record and contact, medical information, etc…

3. a. How will data collected from sources other than Peace Corps records and the volunteer be verified for accuracy?

As part of Infrastructure services we ensure security to prevent data tamper and unauthorized access as well as disaster prevention.

System/Application owners are responsible for verifying the accuracy of the data in their systems.

b. How will data be checked for completeness?

System patches and operating system updates are tested and verified by the vendors before shipment to us for installation.

For application/systems and databases hosted on the infrastructure systems, system/application owners are responsible for checking data for completeness.

c. Is the data current? How do you know?
One of the primary reasons vendors send out patches and software upgrades is to ensure that their systems are up-to-date and current.

For systems and databases hosted on the infrastructure systems, System/Application owners manage the data and ensure it is current.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes, vendor supplied patches and upgrades are documented by the vendor.

For application/systems and databases hosted on the infrastructure systems, this process is managed by the System/Application owners

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Infrastructure systems are access by various staff members depending on job function and need. The different types of system users vary from system administrators who oversee the hardware and operating system to application owners and users. Access is controlled by job function and need.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and

responsibilities regarding access documented?
Yes, access procedures are control through the Personnel Tracking System and the helpdesk. Peace Corps policy MS 542 provides details on system access policy.
3. Will users have access to all data on the system or will the users access be restricted? Explain.
User access is restricted based on job roles and responsibilities.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
Password protection, audit logging and monitoring, end-user security awareness, intrusion detection systems, and firewalls.
5. a. Do other systems share data or have access to data in this system? If yes, explain.
Vendor supported anti-virus software and vendor patches

For business applications hosted on the infrastructure, there are some external interfaces with USDA NFC for payroll systems and the Office of Personnel Management for security systems, and the Treasury and the State departments for financial systems.
b. Who will be responsible for protecting the privacy rights of the volunteers and employees affected by the interface?
For application/systems and databases hosted on the infrastructure systems, this is managed by the System/Application owners.

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
We do not share our operating systems or office support software.

For application systems and databases hosted on the infrastructure systems there are Federal agencies with certain restricted access.

b. How will the data be used by the agency?
Vendor O/S and firmware is used to provide computer services to the agency.

For applications/systems hosted in infrastructure equipment this varies depending on the application/system or database.
c. Who is responsible for assuring proper use of the data?
For O/S and firmware usage the CIO office is responsible.

For systems and databases hosted on the infrastructure systems the system/application owners are responsible.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Yes

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? No

b. Will the new data be placed in the individuals record (volunteer or employee)? No

c. Can the system make determinations about volunteers or employees that would not be possible without the new data? No

d. How will the new data be verified for relevance and accuracy?

For application/systems and databases hosted on the infrastructure systems the system/application owners are responsible.

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Password protection, audit logging, end-user security awareness measures, intrusion detection systems and firewalls

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. Yes, the same controls are applied to the new consolidated environment.

4. How will the data be retrieved? Infrastructure O/S and firmware is not retrievable. Can it be retrieved by personal identifier? If yes,

explain. What are the potential effects on the due process rights of volunteers and employees of:

consolidation and linkage of files and systems; N/A

derivation of data; N/A

accelerated information processing and decision making;

use of new technologies. N/A

How are the effects to be mitigated? N/A

Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of volunteers and employees.

We currently provide limited computer services to Peace Corps volunteers at our overseas administrative offices and for returned Peace Corps volunteers at our domestic regional recruitment offices that provide Internet access and general correspondence capability. All of the applications and systems that are hosted on the infrastructure systems are for administrative support functions. Volunteers do not need access to these systems to fore fill their mission in the field.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? The same polices and operating procedures are used everywhere to manage and maintain our computer systems.

c. Explain any possibility of disparate treatment of individuals or groups.

2. a. What are the retention periods of data in this system? The retention period differs by application/system and database. General office files and emails are retained for three (3) months. All other systems have they own retention schedule. (Please refer to the application/system documentation for details on each system.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

The Infrastructure operating procedure manuals have the documented procedures for archiving and data retention.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

For application/systems and databases hosted on the infrastructure systems the system/application owners are responsible.

3. a. Is the system using technologies in ways that the Peace Corps has not previously employed (e.g. Caller-ID)? No

b. How does the use of this technology affect volunteer/employee privacy? No, impact

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. Yes, through user authentication and system monitoring we do have the capability to identify, locate and monitor activity on the infrastructure network.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain. Yes, at a high level we can based on office assignment codes and user security level. We do not have group policy setting under the NT Domain, but will have this capability available once we moved to Active Directory.

c. What controls will be used to prevent unauthorized monitoring?
The network is monitored by our network security vendor NETSEC. They provide Intrusion detection services and firewall monitoring. These same services are used to prevent unauthorized monitoring.

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

b. If the system is being modified, will the SOR require amendment or revision? Explain.. NO