Privacy Impact Assessment: Telecommunications Systems

FISMA
Privacy Questions

Peace Corps Template of PIA

Data in the System

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

Volunteers & Employees – telephone numbers and IP addresses
Others (Staff) – telephone numbers, IP addresses, and Call Detail Records(CDR)

2. What are the sources of the information in the system?
   a. What Peace Corps files and databases are used?
   b. What Federal Agencies are providing data for use in the system?
   c. What State and Local Agencies are providing data for use in the system?
   d. What other third party sources will data be collected from?
   e. What information will be collected from the volunteer/employee?

Original data stored in PBX Assigned Extension File, VPN Server static IP Address File, CDRs stored in ECAS data file and on read only CD.
No other Federal Agencies are provided access to these files
No State or Local agencies are provided access to these files
Data (CDRs) will be collected from Verizon, MCI, and cisco
No information will be collected from the volunteer/employee

3. a. How will data collected from sources other than Peace Corps records and the volunteer be verified for accuracy?
   b. How will data be checked for completeness?
   c. Is the data current? How do you know?

CDR data is checked for accuracy at the source. Peace Corps does not re-verify the accuracy of the data unless a discrepancy is noted.

CDR data is checked for completeness at the source.
The data is provided to us 30 to 90 days in arrears. CDR records are date/time stamped.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
Telephone numbers and IP Addresses are not described in detail. CDR records are described in detail in their Operations Guide

Access to the Data

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

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?
Access to original sources are protected. Access to PBX administrative files, VPN router administrative files, and CDR files are strictly controlled within the Telecommunications Systems Division. Access is on a need-to-know basis based on personal recognition.

3. Will users have access to all data on the system or will the users access be restricted? Explain.
Users will only access secondary source information such as on-line directories, printed directories and the like. Users do not have access to source data. That information is physical access and password protected.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
The number of people with access is very small. Physical access to the area where the data are stored is monitored by the Telecommunications Systems Division. The data are segregated such that access to one set of files – PBX assigned extensions for example – does not also provide access to IP addresses. No other restrictions exist for authorized access to telephone number and IP address lists. Access to CDR's is restricted within the Telecommunications Systems Division to a small number of people. There are no further restrictions – in particular, browsing the data is one of the tasks of the authorized user to search for anomalies.

5. a. Do other systems share data or have access to data in this system? If yes, explain.
No

b. Who will be responsible for protecting the privacy rights of the volunteers and employees affected by the interface?
The Telecommunications Systems Division

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
No

b. How will the data be used by the agency?
Telephone number and IP address information will be used by the agency to provide volunteers and employees electronic addresses for access by automated systems. CDR data is used to develop chargeback and future budgets.

c. Who is responsible for assuring proper use of the data?
Telecoms Manager

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?
Telephone number and IP address data will be checked both automatically by the systems and manually by Administrative forces for relevance and accurary

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
CDR data is being consolidated and is being protected by a combination of physical access limitations and passwords.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
Yes. A combination of physical access limitations (the consolidated information will not be available on the Intra- or Inter- Nets), recognition (only people recognized as Telecommunications Systems Administrators will be

allowed to access the terminal), and passwords at the terminal will prevent unauthorized access.

4. How will the data be retrieved? 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;
derivation of data;
accelerated information processing and decision making;
use of new technologies.

How are the effects to be mitigated?

CDR data can be retrieved and analyzed based on any of the over 100 field names, including telephone number. Data cannot be accessed by personal identifier. The external records of business telephone and data calling is not private information and is commonly used in aggregated form for charge back and future budget analysis.

Since the CDR data addresses message externals, the opportunity for accelerated processing and / or new technology will not have an impact on due process rights of employees and volunteers since personal information is not involved.

Maintenance of Administrative Controls

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

The system and its use regarding CDRs will address aggregate entities, not individuals. Organizations of employees and volunteers will be affected primarily for purposes of chargeback and there will be administrative regulations put in place to ensure equitable treatment across organizational lines.

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 CDR analysis process will operate at one site only.

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

NA

2. a. What are the retention periods of data in this system?

Telephone numbers and IP addresses are associated with offices and computers and change as people move. The retention period for CDRs is three years.

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

System save processes automatically eliminate data as the appropriate time arrives. Since the CDR process is new, the procedures for data retention and elimination are being developed now and will be ready by the time the system begins operations.

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?
The CDR data arrives as a read-only file and the source data remains in that state. During the time the data is processed for charge back and budget analysis, typically over the course of two months, the information will not age.

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?
Neither by use of telephone numbers and IP addresses nor by analysis of CDR data is volunteer / employee privacy affected.

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
No

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
No

c. What controls will be used to prevent unauthorized monitoring?
The telephone switches are in protected environments with only limited, authorized access. Devices cannot be placed on the switches without prior approval of the Telecommunications Systems Division. The telecommunications industry has strict regulations concerning what can be attached to the network.

The Peace Corps presently depends on volume to protect cellular systems from monitoring.

Since the CDR data will not be transmitted, it cannot be illicitly monitored.

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.