Privacy Impact Assessment: Peace Corps Intranet

FISMA

PRIVACY QUESTIONS

Data in the System

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

The Peace Corps Intranet does not maintain any Volunteer records and is not generally available to the Volunteers. However, the intranet may have content published by the Intranet Editors that may list specific Volunteer information and related activities, such as the bi-weekly Messenger article.

The Peace Corps Intranet is a one stop portal for several web applications that assist employees. Common examples include the Staff Directory to search for employee information and the TimePeace to enter and report Time and Attendance information. All employees need to have user-id to log in to access the Intranet. Encrypted passwords are stored in an Oracle database.

Other information includes content from various offices and units, and reference pages from several other agencies and federal sites.

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?

The intranet has policy and reference information such as the Peace Corps Manual Section, Medical Technical Guidelines, news and articles such as the press clips, etc. All files, documents and web content are managed and displayed using a Cold Fusion interface and supported via a back end (WEBPRD) Oracle database.

Most of the information is authored and published by the Intranet Editors, and each business unit has one or more designated staff to perform this activity. The site has links to other federal sites for best practices, reference data and essential forms, such as from opm.gov, and the state department (dos.gov) for overseas travel information. Although not restricted, to the best of our knowledge there are no reference links to the State and Local agencies on the Intranet.
The primary intent of the intranet is to serve the Peace Corps employees only and is not available to other third party sources. Besides the reference, news and related articles, there is no mechanism to directly collect data from any third party resources.

The intranet is generally not available to the Peace Corps Volunteers. On a periodic basis electronic surveys are conducted to get feedback from Volunteers and employees. The results of these surveys are hosted on the Intranet. In addition to the survey data, news related content is published in the Messenger article and daily press clips.

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?

The privilege to publish content on the intranet is restricted to a team of Intranet Editors. It is the responsibility of the editors to ensure the content is safe, accurate and follows the styles and guidelines of the site. There is an approval workflow in place to ensure consistency. After the Intranet Editor creates the web content, the Intranet Administrator has to provide the final approval to publish this content on the intranet. As previously stated, the responsibility to keep the content fresh and current as well as the accuracy and completeness stays with the Intranet Editor, who is essentially the designated author of the content.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

The guidelines and content styles for publishing on the intranet which is primarily used to create content is documented in
http://inside.peacecorps.gov/index.cfm?viewDocument&document_id=2072&filetype=htm (Peace Corps Style Guidelines).
The intranet application design, database schema and the data elements are documented in detail and stored as part of the ASD developer documentation. This document is of no

value to the Peace Corps employees and access is restricted to the ASD developer team. The name of the document is **ColdFusion Application System Technical Documentation for *Intranet*** and **Application Operations Manual for *Intranet Interface Programs.***

Access to the Data

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

Content and data published for all (general use) is available to all registered users of the Intranet that comprises of Peace Corps employees – users, managers, system administrators, developers and other staff. However content can be restricted and made visible to certain groups that may be defined in the system. The content can only be modified (insert, delete, update) by the Intranet Editors, and typically each business unit designates one or more employees to play this role. The Intranet Administrator from the OCIO office has extended publishing privileges and can create and assign groups for the intranet. The ASD developers may be assigned privilege to access the application software code and design documentation to enhance and maintain the system. Likewise the ASD database administrator has access to the oracle database to maintain and support the backend database operations.

.

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

All registered users on the intranet have access to the web content via the "User" access level. This level gives the registered user access to all data that is not otherwise set aside for privileges access. The Site Management tool is used for content management. This tool has other levels of access namely Editor, Approver and Admin. These access privileges are granted and managed via the Access Policy in the (BizApps) Application registry. The technical documentation for the Site Management Tool and the BizApps Application registry provides the required details on the user access control and process management.

3. Will users have access to all data on the system or will the users access be restricted? Explain.

All registered users on the intranet have access to the web content via the "User" access level. This level gives the registered user access to all data that is not otherwise set aside for privileges access. Content can be restricted and made visible to certain groups that may be defined in the system. The content can only be modified (insert, delete, update)

by the Intranet Editors, and typically each business unit designates one or more employees to play this role.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

The Manual Section MS 542 enforces the IT Security Policies and Procedures. The intranet system is designed to include access controls. These controls are used by the content rendering engine to display web pages that have passed the access credentials of the user logged into the system. Data access controlled by this process eliminates or minimizes the risk of misusing the data. At the database level audit log of last update is maintained for all Editors who have such access to the system.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

In general other systems do not share or have access to the Intranet system. However, the login authentication module that provide user access to the system is a common framework across all Biz Apps (web based applications).

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

The responsibility for protecting the privacy rights of the volunteers and the employees is not any different than other IT systems in the agency. All guidelines and procedures set in the Peace Corps Manual Section MS 542 on Peace Corps IT Security Policies and Procedures are applicable to the Intranet as well.

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

At this time it is not anticipated that other agencies need access to the intranet content and data.

b. How will the data be used by the agency?
Information resources for daily activities.

The intranet provides a portal front end to the Staff Directory to search for employee information and the TimePeace to enter and report Time and Attendance information. Other common links that are hosted on the site include Odyssey Financial applications. PC Manual Chapters and Medical Technical Guideline provide reference points for PC employees.

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

The Manual Section MS 542 enforces the IT Security Policies and Procedures. The intranet system is designed to include access controls. . These controls are used by the content rendering engine to display web pages that have passed the access credentials of the user logged into the system. Data access controlled by this process eliminates or minimizes the risk of misusing the data. At the database level audit log of last update is maintained for all Editors who have such access to the system.

All registered users on the intranet have access to the web content via the "User" access level. This level gives the registered user access to all data that is not otherwise set aside for privileges access. The Site Management tool is used for content management. This tool has other levels of access namely Editor, Approver and Admin. These access privileges are granted and managed via the Access Policy in the (BizApps) Application registry.

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, the intranet provides a portal front end to the Staff Directory to search for employee information and the TimePeace to enter and report Time and Attendance information. Other common links that are hosted on the site include Odyssey Financial applications. PC Manual Chapters and Medical Technical Guideline provide reference points for PC employees.

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

The intranet doesn't derive new data or create previously unavailable data about on individual.

b. Will the new data be placed in the individuals record (volunteer or employee)?

The intranet doesn't place new data in the individuals records.

c. Can the system make determinations about volunteers or employees that would not be possible without the new data?

The intranet doesn't derive new data or create previously unavailable data about on individual.

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

Revelance of content determine by Editor designated by offices.

3. a. If data is being consolidated, what controls are in place to protect the data

from unauthorized access or use?

The intranet doesn't consolidate data.

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

No processes on intranet being consolidated.

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?

The Manual Section MS 542 enforces the IT Security Policies and Procedures. The intranet system is designed to include access controls. . These controls are used by the content rendering engine to display web pages that have passed the access credentials of the user logged into the system. Data access controlled by this process eliminates or minimizes the risk of misusing the data. At the database level audit log of last update is maintained for all Editors who have such access to the system.

Maintenance of Administrative Controls

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

The Peace Corps Intranet does not maintain any Volunteer records and is not generally available to the Volunteers. However, the intranet may have content published by the Intranet Editors that may list specific Volunteer information and related activities, such as the bi-weekly Messenger article.

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 Peace Corps Intranet is not operated in more than one site.

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

All registered users on the intranet have access to the web content via the "User" access level. This level gives the registered user access to all data that is not otherwise set aside for privileges access. The Site Management tool is used for content management. This tool has other levels of access namely Editor, Approver and Admin. These access privileges are granted and managed via the Access Policy in the (BizApps) Application registry.

Content and data published for all (general use) is available to all registered users of the Intranet that comprises of Peace Corps employees – users, managers, system administrators, developers and other staff. However content can be restricted and made visible to certain groups that may be defined in the system. The content can only be modified (insert, delete, update) by the Intranet Editors, and typically each business unit designates one or more employees to play this role. The Intranet Administrator from the OCIO office has extended publishing privileges and can create and assign groups for the intranet. The ASD developers may be assigned privilege to access the application software code and design documentation to enhance and maintain the system. Likewise the ASD database administrator has access to the oracle database to maintain and support the backend database operations.

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

Intranet client access cookies expire after 17 days. Client variables contained login information, last date visited are getting cleared up every 24 hours of user's inactivity. Content data in the Oracle database that entered by Editors can be edited or deleted by them, as well as saved indefinitely.

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

Intranet client access cookies expire after 17 days. Client variables contained login information, last date visited are getting cleared up every 24 hours of user's inactivity. Content data in the Oracle database that entered by Editors can be edited or deleted by them, as well as saved indefinitely.

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?

Intranet client access cookies expire after 17 days. Client variables contained login information, last date visited are getting cleared up every 24 hours of user's inactivity. ColdFusion code controls lifetime of variables and cookies.

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?

Intranet doesn't effect volunteer/employee privacy.

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

System enable user to identify individual by using Staff directory.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

System enable user to identify individual by using Staff directory.

c. What controls will be used to prevent unauthorized monitoring?

All registered users on the intranet have access to the web content via the "User" access level. This level gives the registered user access to all data that is not otherwise set aside for privileges access. The Site Management tool is used for content management. This tool has other levels of access namely Editor, Approver and Admin. These access privileges are granted and managed via the Access Policy in the (BizApps) Application registry. The technical documentation for the Site Management Tool and the BizApps Application registry provides the required details on the user access control and process management.

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

The intranet application design, database schema and the data elements are documented in detail and stored as part of the ASD developer documentation. This document is of no value to the Peace Corps employees and access is restricted to the ASD developer team. The name of the document is **ColdFusion Application System Technical Documentation for *Intranet*** and **Application Operations Manual for *Intranet Interface Programs.***

b. If the system is being modified, will the SOR require amendment or revision? Explain.

The intranet application design, database schema and the data elements are documented in detail and stored as part of the ASD developer documentation. This document is of no value to the Peace Corps employees and access is restricted to the ASD developer team. The name of the document is **ColdFusion Application System Technical Documentation for *Intranet*** and **Application Operations Manual for *Intranet Interface Programs.***