# Privacy Impact Assessment: Bizapps

**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.

Employee, Payroll (including time and attendance), Volunteer, Prospect and web content.

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 majority of the data is entered by Peace Corps staff using Bizapps and other Peace Corps business applications. Data is stored in the main Oracle database residing on the mainframe and in the Oracle web database which serves the intranet and public web sites. A small amount of data is affected by outside sources such as the National Finance Center from which we download personnel data each pay period. Detailed information beyond the general description in #1 would need to be provided by each Bizapp Application owner.

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 data for many of the Bizapps is shared with other Peace Corps applications thus, the accuracy and completeness, is dependant upon the other applications and the nature of the data involved.

One control for Bizapps access is the removal of all Bizapp application access when a staff person is flagged as terminated in PTS. PTS data accuracy is helped by the recently introduced, PTS Data Quality Assurance program. This program runs several tests daily and emails responsible POC's about potential data issues. The POC receive an email about the problem each day until it is resolved. Monthly reports on these data issues and reviewed to detect problem areas. PTS and TimePeace data are also synced with data downloads from NFC each pay period. Since NFC is the official personnel and payroll system for Peace Corps, this makes our data as accurate as the official record.

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

This question is application dependant.

**Access to the Data**

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

Each Bizapp has a defined access policy and users should only be granted access to each application according to that policy. In addition, developers and other CIO staff may have direct access to the database due to their position.

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

See #1 above. In addition each business owner may have policy, procedures and controls in place to manage who they request access for.

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

Data access within each Bizapp can be managed using the defined access levels. Access levels are set when access is granted. Some Bizapps, TimePeace in particular, use additional controls to determine access.

For example, all TimePeace users begin with the "USER" access level. Administrators are switched to the "ADMIN" using the Bizadmin application. Supervisor access is determined by whether the person is set as the supervisor of any other active staff person in PTS. And timekeepers are defined using a separate function within the TimePeace administrator module.

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

Each Bizapp connects to the database as it's own Oracle user. Each Oracle user only has priviledges  to the specific tables and objects that it needs to function. Beyond that a person would need access to the database including user and password information. Passwords for each user are kept on a need to know basis and generally knowable to less than a handful of staff at any given time. The passwords are also managed in accordance with the official Peace Corps password policy.

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

          Yes. Peace Corps has many types of business applications and depending on the specific data, it may be shared among many of them.

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

          Application specific.

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

          Application specific.

        b. How will the data be used by the agency?

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

**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?

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

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

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

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

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

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?

**Maintenance of Administrative Controls**

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

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?

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

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

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

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?

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?

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

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

c. What controls will be 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.

Typical PIA

**1. PROJECT IDENTIFICATION**
**IDENTIFICATION INFORMATION**
**PROGRAM OR APPLICATION NAME:**
**APPLICATION FINANCE No: EIR NUMBER:**
**Area/District Manager:**
**Telephone Number:**
**Email Address:**
**FCCO Manager:**
**Telephone Number:**
**Email Address:**
**ITPC Manager:**
**Telephone Number:**
**Email Address:**
**ISSO:**
**Telephone Number:**
**Email Address:**
**Privacy Official:**
**Telephone Number:**
**Email Address:**
**DEVELOPMENT AND PRODUCTION INFORMATION**
**Development Organization:**
**Development Site:**
**Production Site(s):**
**Summary Description of the proposed System:**
**Production Date:**

**2. PRIVACY COMPLIANCE**
**2-1 SYSTEM OF RECORDS – Data Management Yes No**
Does the program or application collect or store information related to a customer or employee
where data is retrieved by name, unique number, symbol, or other identifier assigned to the
customer or employee?
**2-2 NOTICE Yes No**
Is information collected directly from a customer or employee?
**2-3 CHOICE Yes No**
Do you intend to use customer information for a secondary marketing use, such as to up-sell
or cross-sell to the customer, or to share the customer's information with third parties for
marketing purposes?
**2-4 SUPPLIERS Yes No**
Are contractors or business partners: 1) employed regarding the application OR
2) helping design, build, or operate a customer-facing web site?
**2-5 WEB SITES Yes No**
Does the application include a customer-facing web site not on usps.com?
**2-6 CHILDREN'S ONLINE PRIVACY PROTECTION ACT Yes No**
If an online customer site, does it identify ages or is it directed to persons under 13?
**2-7 GRAMM–LEACH-BLILEY ACT – Financial Services Yes No**
Does the application provide a financial service? Examples include banking activities or
functions; wire/monetary transfers; printing, selling, or cashing checks; providing USPS credit
services. It does NOT include payment by check or credit card issued by another entity.
**2-8 PRIVACY RISKS Yes No**
Does the program or application collect or store information related to customers or
employees; involve a customer web site; or use technology that can track customer behavior?
**2-9 DESCRIPTION of INFORMATION MANAGEMENT PRACTICES**
If "YES" was checked for any of the above, please provide a brief explanation for each "YES" item below.

### 3. GENERAL DATA ATTRIBUTES
**3-1 DATA TYPES:**
What data is being collected? (customer, employee, product/service related, none, etc.)
**3-2 DATA SOURCES:**
Who provides the data?
**3-3 DATA ACCESS:**
Who has access to the data?
**3-4 DATA SHARING:**
Will the data be shared externally? If so, with whom?

### 4. DETERMINATION OF SENSITIVITY
**4-1 Data Element Sensitivity Designation**
**4-1.1 Personal Data**
**SENSITIVE**
full Social Security number fingerprints info held for law enforcement purposes
biometric data other: address change w/court ordered non-disc.
**BUSINESS-CONTROLLED SENSITIVITY**
home street address* home phone number * personal cell phone number *
birth date/age* partial Social Security driver's license number
credit card # (full or partial) race/national origin* change of home address*
other account number marital status* customer obtained demographic info.*
family information buying habits* externally obtained demographic info.*
web navigation habits* bill payee name bill payee address
bill payee phone number bill payee acct number bank routing number
bank account number personal email address personal clubs & affiliations*
income/assets: photographs other:
*Data element with a name or personal identifier is business-controlled sensitivity.*
*Data element without a name or personal identifier is nonsensitive.*
**NONSENSITIVE**
Name city, state, & zip (H or W) work street address
work phone number work fax number work cell number
work pager number work email address Occupation
job description USPS salary professional affiliations
ICQ/chat address IP address Gender
USPS employee ID number USPS emp. position (title other:
**4-1.2 Business Data**
**SENSITIVE**
national security related
information
communications protected by
legal privileges
USPS restricted financial/trade
secrets/proprietary
other:
**BUSINESS-CONTROLLED SENSITIVITY**
not publicly available USPS
documents
not publicly available info
from business partners
other:
**NONSENSITIVE**
publicly available USPS
information
publicly available info from
business partners
other:
**4-2 Impact of Unauthorized Use**
**1. Is the data subject to potential fraud or manipulation for financial gain? Check one.**
Info has little or no potential to be used for financial gain through fraud or manipulation. **NS**
Info has moderate potential to be used for financial gain through fraud or manipulation. **BCS**

Info has significant potential to be used for financial gain through fraud or manipulation. **S**
**2. What is the impact on USPS of unauthorized disclosure or misuse of the information?**
Unauthorized disclosure/misuse of info would result in little or no financial loss/negative impact to brand. **NS**
Unauthorized disclosure/misuse of info would result in moderate financial loss/negative impact to brand.
**BCS**
Unauthorized disclosure/misuse of info would result in significant financial loss/negative impact to brand. **S**
**3. What is the impact on the individual on whom information is maintained if unauthorized disclosure or**
**misuse of information occurs? Check one.**
Results in little or no harm, embarrassment, inconvenience, or unfairness to individual. **NS**
Results in moderate harm, embarrassment, inconvenience, or unfairness to individual. **BCS**
Results in significant harm, embarrassment, inconvenience, or unfairness to individual. **S**
**4-3 SENSITIVITY DETERMINATION SUMMARY**
Based on evaluation of the responses and type of info being collected, application is designated as:
**Nonsensitive**
**S iti**
**N**
**Business-Controlled Sensitivity**
**S iti N**
**Sensitive**


**CRITICALITY DETERMINATION**
**Noncritical Business-Controlled Criticality Critical**
**5. GENERAL APPLICATION DATA**
This section will be used later if the Information Security Assurance (ISA) process requires security controls to protect
the application.
**5-1.1 General Information**
Name of Application
URL of website (if applicable)
Description:
IP address(s)
Hostname(s)
EIR#
Business Owner:
Governing Office:
Webmaster:
Reason for Application
**5-1.2 Technical Information**
Application Software – ((Version & Service Pack)
Operating System – (Version & Service Pack)
HTTP Server Software (Type & Version)
Database (Type & Version)
Dynamic HTML? (Type & Version)
Remote Management?
508 Compliant?
External links, Ad Banners?
**5-1.3 HCS Information**
Login/Password required?
OS patches applied? (Include Date):
Application patches applied? (Include Date):
Database Hardened?
Server Hardened?
Backups Performed Onsite & stored Offsite?
APPENDIX B – BIA SHORT FORM
August 2004 5


**6. NETWORK CONNECTIVITY CHARACTERISTICS**
**Question Yes No**
1. Will the application utilize connections via Internet including Postal-to-Postal (e.g., cable or
DSL)?

2. Will the application require a change to a perimeter firewall configuration?
3. Will the application require a change to a secure enclave firewall configuration?
4. Will the application utilize a wireless LAN, wireless access point, or wireless devices such as PDAs?
5. Will the application access development, production, or internal Postal networks via the Internet or Internet connectivity?

**7. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY**
**7-1.1 Area/District Manager**
I am responsible for funding and procuring, developing, and integrating privacy and security controls that
will satisfy the information security requirements (identified above) in accordance with the ISA process
outlined in Handbook AS-805-A, *Application Information Security Assurance Process,* and, if applicable,
Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment.* I
understand that compliance with the ISA process may affect the development time and cost of this
project and must be planned for accordingly. I will ensure that Postal Service privacy and information
security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.

**ISSO Recommendation:**
**Comments:**
**Signatures:**

_____ _____
Business Owner Date (MM/DD/YYYY)
_____ _____
FIS Manager Date (MM/DD/YYYY)
_____ _____
ISSO Date (MM/DD/YYYY)
_____ _____
Privacy Official Date (MM/DD/YYYY)

## **FISMA Requirements**

Section D - Reporting Template for Senior Agency Officials for Privacy

A reporting template tool will be sent at a later date. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

I. Senior Agency Official for Privacy Responsibilities

1. Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)?
Yes or No.

2. Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19?
Yes or No.
3. Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information?
Yes or No.

II. Procedures and Practices

1. Does your agency have a training program to ensure that all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?
Yes or No.

2. Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)? Yes or No.

3. Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act.
Please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year.
[make chart with the following headings]

| Section M Contracts | Records Practices | Routine Uses | Exemptions | Matching Programs | Training | Violations | Systems of Records |
|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |

4. Section 208 of the E-Government Act requires that agencies (a.) conduct Privacy Impact Assessments under appropriate circumstances, (b.) post web privacy policies on their websites, and (c.) ensure machine-readability of web privacy policies.
a. Does you agency have a written process or policy for:
    (i) determining whether a PIA is needed? Yes/No
    (ii) conducting a PIA? Yes/No
    (iii.) evaluating changes in business process or technology that
    the PIA indicates may be required? Yes/No
    (iv.) ensuring that systems owners and privacy and IT experts
    participate in conducting the PIA? Yes/No
   (v.) making PIAs available to the public in the
    required circumstances? Yes/No
    (vi.) making PIAs available in other than required circumstances? Yes/No

b. Does your agency have a written process for determining continued compliance with stated web privacy policies?
Yes or No.
c. Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)?
Yes or No.
(i.) if not, provide date for compliance:

5. By bureau, identify the number of information systems containing Federally-owned information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?
   a. FY 05 Systems that contain Federally-owned information in an identifiable form
- By bureau: number that contain information in an identifiable form
   o Agency Systems
   o Contractor Systems
   o Total number of systems

   b. FY 05 Privacy Impact Assessments
- By bureau: total number requiring a Privacy Impact Assessment in FY 05 (systems that are new or have been substantially altered)
   o Agency Systems
   o Contractor Systems
   o Total number of systems
- By bureau: number that have a completed Privacy Impact Assessment within FY 05
   o Agency Systems
   o Contractor Systems
   o Total number of systems

   c. FY 05 Systems of Records Notices
- By bureau: number of systems from which Federally-owned information is retrieved by name or unique identifier
   o Agency Systems
   o Contractor Systems
   o Total number of systems

- By bureau: number of systems for which one or more Systems of Records Notice/s have been published in the Federal register
   o Agency Systems
   o Contractor Systems
   o Total number of systems

   d. Contact Information for preparer of question 5.

6. OMB policy (Memorandum 03-22) prohibits agencies from using persistent tracking technology on web sites except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

    a. Does your agency use persistent tracking technology on any web site? Yes/No

    b. Does your agency annually review the use of persistent tracking? Yes/No

    c. Can your agency demonstrate through documentation the

    continued justification for and approval to use the persistent technology? Yes/No

    d. Can your agency provide the notice language used or cite to the web privacy

    policy informing visitors about the tracking?

    Yes or No.

III. Internal Oversight

1. Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies?

Yes or No.

(i.) If so, provide the date the documentation was created.

2. Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies?

Yes or No.

(i.) If so, provide the date the documentation was created.

3. Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices?

Yes or No.

4. Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:

    a. compilation of the agency's privacy and data protection policies and procedures?
    Yes/No

    b. summary of the agency's use of information in identifiable form? Yes/No

    c. verification of intent to comply with agency policies and procedures? Yes/No

5. Does your agency submit an annual report to Congress (OMB) detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred?

Yes or No.

(i.)If so, when was this report submitted to OMB for clearance?

IV. Contact Information

Please provide the names, phone numbers, and e-mail addresses of the following officials:

Agency head:

Chief Information Officer:

Agency Inspector General:

Chief Information Security Officer:

Senior Agency Official for Privacy:

Chief Privacy Officer:

Privacy Advocate:

Privacy Act Officer:

Reviewing Official for PIAs: