DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Internet Based Registration Service (IBRS)
Updated April 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Email: PIA@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?**

YES _X__ NO___

**** “Personally identifiable information from/about individual members of the public” means personally identifiable information from/about “any person not acting in his/her official capacity as a federal government employee/contractor”.**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail address: PIA@state.gov

2) Does a Privacy Act system of records already exist?

YES __X_ NO___

If yes, please provide the following:
System Name Overseas Citizen Services Records Number STATE-05

If no, a Privacy system of records description will need to be created for this data.

3) What is the purpose of the system/application?

The IBRS is a service of the American Citizen Services (ACS) program. The ACS program consists of a suite of tools for tracking and managing information pertaining to American citizens abroad. The IBRS allows American citizens to provide travel registration information electronically over the Internet via appropriate secure connections. The IBRS application accepts information from American citizens through the Internet, creates cases within the registration service, and replicates the information to the appropriate post(s). Additionally, IBRS has the capability of transferring its data to to users will be able to access IBRS data through the CCD portal reporting capability.

From the Internet based users perspective, the functionality of the IBRS web site will be relatively simple. Users will access the IBRS web site and be provided with an overview of registration, and instructions on how to register. Individuals registering in IBRS have the option of creating a user account, and, if so, will provide a username and password. If users wish to return to the website to change any of the provided information, they must choose the option to create an account and will use their username and password to access the site, edit their data, and re-submit the form. Once authenticated to the system by username and password, these users will access a secure form through a series of screens, fill out the form, and submit it. At that point, the user has registered. An additional function that will be supported beyond the basic registration scenario includes display and distribution of travel warnings and other to registrants, data retrieval and reporting functions for consular personnel, and web site administration functions.

The Consular Task Force (CTF) subsystem has recently been added to IBRS. The CTF subsystem is used by the Department of State to provide assistance and information to American citizens overseas when a crisis occurs. CTF gives the DoS user the capability to create and maintain a running log of events associated with the crisis at hand to use to inform concerned family members, friends, members of Congress, and others who need to learn the status of the crisis situation and the welfare and whereabouts of particular crisis participants.

The major business functions of CTF are:

- Talking Point - the Talking Point function allows the task force coordinator to create and maintain informational documents related to the crisis for use by task force personnel.
- Subject – the Subject is the American Citizen (AMCIT) involved in the crisis. The Subject function in CTF provides for recording and maintaining identifying information regarding the AMCITS involved in the crisis.
- Contact - the Contact can be any individual calling to inquire about the status of an AMCIT involved in a crisis. The Contact function in CTF provides for recording and maintaining identifying information regarding the contact.
- Call Back - the Call Back function allows the task force to record and manage activities related to contacting the Contacts with additional information regarding the status of the AMCIT involved in the crisis.
- Action Item - the Action Item function allows the task force coordinator and CTF users to maintain the list of action items that need to be accomplished per task force shift.
- Management Function - this function allows the task force coordinator and system management personnel to manage basic system activities, i.e. managing the user table, managing validation tables, running reports, etc.
- Super Search/Group Cable - this function provides the task force users with expanded query and reporting capabilities along with the ability to generate group telegrams.

4) What legal authority authorizes the purchase or development of this system/application?

22 U.S.C. 2715 and 7 FAM 042. If a major disaster or incident abroad occurs which affects the health and safety of citizens of the United States residing or traveling abroad, the Secretary of State shall provide prompt and thorough notification of all appropriate information concerning such disaster or incident and its effect on U.S citizens to the next-of-kin of such individuals.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

U.S. Citizens: U.S. citizens are the primary individuals covered by the systems under this program.

Non-U.S. Citizens: Some non-U.S. citizen data may be collected in the process of providing services. For example, non-citizen relative information, contact information or service provider information may be collected during the process of providing services to American citizens abroad.

DoS employee information such as a name is collected and stored with the applicant's record as it relates to the auditing of actions taken during the processing of the applicant's service request.

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

a. Who/what is the source of the information?

For IBRS, the primary source of information is from public Internet users; this includes travel agents representing groups of travelers and individual registrants. Consular users can also create new registration records on a traveler's behalf if they do not have access to the Internet.

For CTF, information comes directly from the two CTF user groups: CTF caseworkers and managers.

b. What type of information is collected from the source of the information?

For IBRS, information collected from the public includes data relevant to registration of travel abroad. In almost all cases, personal biographic data, such as a name, passport number, address, phone number, emergency contact information, and itinerary information, etc. is collected. The following information is *required* to register within IBRS:

- Country Visiting;
- Destination Date of Arrival;
- Destination Date of Departure;
- Traveler First Name;
- Traveler Last Name; and
- Traveler's date of birth ().DOB

For CTF, information collected from caseworkers and managers includes information regarding the crisis and the data relevant to the American citizens (subjects) involved in the crisis, other subjects related to them, either by family or affiliation (related subject), and the concerned relation who calls in about the subject (contact). The following information is *required* within CTF:

- Subject's last name;
- Subject's gender;
- Subject's last known whereabouts;
- Contact's first name;

- Related subject’s last name;
- Related subject’s gender;
- Official name of the crisis event;
- Beginning date of crisis event; and
- Talking points to read to inquiring callers.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

IBRS uses JavaScript validation and input masks on the client side to ensure that users input valid and complete information into form fields. In addition**,** post overseas staff validates the record of each IBRS Internet based user. Validation reduces the number of false records in the system and ensures the correct post is managing the record.

Input accuracy for CTF is controlled through user roles. Non-manager users cannot set up crisis’ or set talking points within CTF. Caseworker data input is mainly restricted through the use of drop down menus on tabs to which they have access. Once a user role is parsed, only the tabs the user has edit privileges to are revealed on screen.

b. How will data be checked for completeness?

Both IBRS and CTF call for a minimum number of required fields to be completed. For IBRS, users are prevented from continuing the registration process unless the information gathered meets specified standards. For CTF, the data pulled from IBRS is considered complete. Required fields within IBRS and CTF are in Section 2b of this document.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Within IBRS, the users’ personal data will remain in active files for 12 months after the completion of their last trip, their last registration activity, or their departure date from their foreign country of residence. At that time, the user will receive an e-mail notifying them that their registration data records, log-on, and password will be automatically deleted after three months unless they take steps to keep their registration active. No data from the IBRS system will be archived. Indefinite registrations of long-term residents abroad will remain in the file unless edited or deleted by the registrant.

For CTF, when a crisis has ended, all user accounts will be turned to a status of “inactive.” The user will still have access to the CTF application, but they will not be able to add new data.

D. <u>INTENDED USE OF THE DATA:</u>

1) **Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?**

   Yes, the use of data within IBRS and CTF is both relevant and necessary to the purpose for which the systems were designed.

2) **Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

   For IBRS, no new data or previously unavailable personal data will be created through derived data or aggregation of data collected. However, records created within the IBRS system are replicated into the Consular Consolidated Database (CCD). Once thedata is aggregated in CCD, it serves as both a backup for each post's transaction activity, and it allows the Bureau of Consular Affairs management the ability to apply advanced metrics against the data. Whenever a record is updated within IBRS, the information is replicated into the CCD where it is maintained.

   For CTF, no new data or previously unavailable personal data will be created through derived data or aggregation of data collected.

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

   Not applicable as no new data is created.

4) **Will the new data be placed in the individual's record?**

   Not applicable as no new data is created.

5) **How will the new data be verified for relevance and accuracy?**

   Not applicable as no new data is created.

6) **How will the data be retrieved?   Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

   With their initial registration, public Internet-based users have the option of creating a username and password that will enable them to access their trip data upon logging into IBRS/CTF.

   Consular users can retrieve registrant data by using the following personal identifiers:

   - Registrant's given name;
   - Registrant's surname; and
   - Registrant's date of birth (DOB).

7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Bureau of Consular Affairs users have the ability to generate predefined reports of the IBRS travel data entered by the registrants based upon selected criteria. Reports are used to help Consular users manage the registration records in the IBRS system, especially in the event of an emergency.

The following reports can be produced on individuals:

- Registrant Contact List Report - provides a complete list of registrants who fit the report criteria. The list of registrants includes contact information in the destination country, emergency contact information (if any), and the privacy waiver selection for each registrant in the list.
- Registrant Email List Report - provides registrant e-mail addresses in a format ready to be inserted into an e-mail message or exported to a spreadsheet.
- Registrant Lookup Report - provides a summary list of registrants from which the user can choose to view a detailed report.
- Registrant Lookup for Multiple Posts Report - provides a summary list of travelers who have registered visits not only at the post selected, but who have also registered for visits to other posts. The user can choose to view a detailed report for each registrant.
- Organization Report - provides a list of the registrants for a particular organization by post or country.
- Marked for Deletion List - provides a summary list of registrants that have been marked for deletion. The user can choose to view a detailed report for each registrant.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

IBRS/CTF is not operated in more than one site; it is operated centrally as a web application.

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

Within IBRS, the public users' personal data will remain in active files for 12months after the completion of their last trip, their last registration activity, or their departure date from their foreign country of residence. At that time, the user will receive an e-mail notifying them that their registration data records, log-on, and password will be automatically deleted after three months unless they take steps keep their registration active. No data from the IBRS system will be archived. Indefinite registrations of long-term residents abroadwill remain in the file unless edited or deleted by the registrant.

Currently,CTF records are stored in the database indefinitely.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Policies/procedures governing the disclosure of American citizen information is specified in various sections in the Foreign Affairs Manual (FAM), volume 7 , Consular Affairs. The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No, the system is not using technologies in ways previously not employed by the Department of State.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

Not applicable as the system is not using technologies in ways previously not employed by the Department of State.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

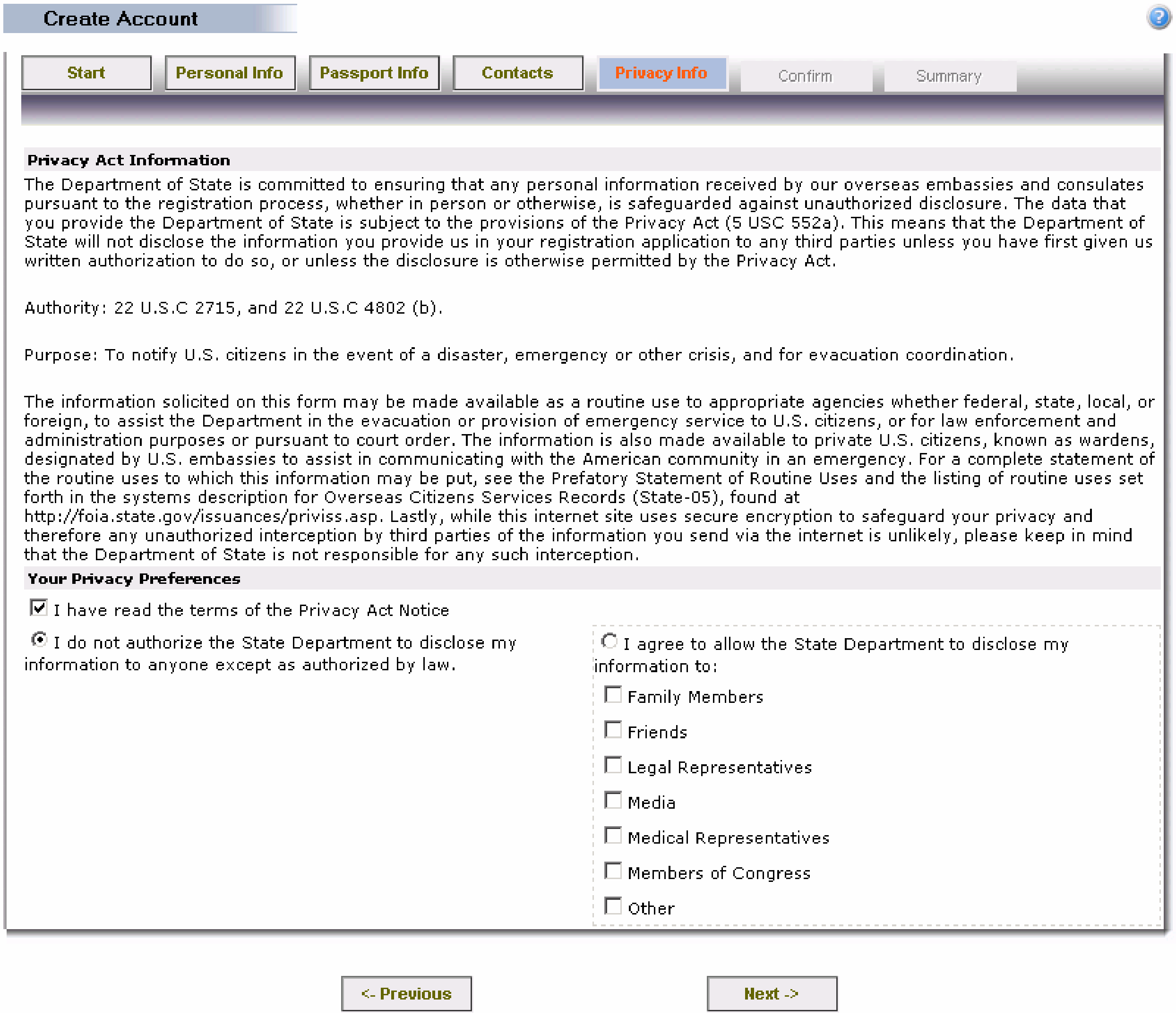
The system is used to identify and locate American citizens abroad in the event of an emergency or crisis situation of which they need to be notified. Basic biographic information provided by the individual is collected as a function of this capability. Physical, technical and management controls are in place to prevent unauthorized monitoring of individuals.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Enhancements were made to the application, but there were no changes to the data collected from the previous version of the application. Therefore, the Privacy Act system of records does not require amendment or revision.

8) **Are there forms associated with the system? YES _X__ NO ___**
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Web forms are used to collect applicant data within IBRS under this program are OMB approved and contain a Privacy Act statement. IBRS requires the user to complete the privacy act notification; registrants are required to indicate that they have read the Privacy Act statement before registering a trip. The Privacy Act statement for IBRS appears as follows:



Privacy Act Information

The Department of State is committed to ensuring that any personal information received by our overseas embassies and consulates pursuant to the registration process, whether in person or otherwise, is safeguarded against unauthorized disclosure. The data that you provide the Department of State is subject to the provisions of the Privacy Act (5 USC 552a). This means that the Department of State will not disclose the information you provide us in your registration application to any third parties unless you have first given us written authorization to do so, or unless the disclosure is otherwise permitted by the Privacy Act.

Authority: 22 U.S.C 2715, and 22 U.S.C 4802 (b).

Purpose: To notify U.S. citizens in the event of a disaster, emergency or other crisis, and for evacuation coordination.

The information solicited on this form may be made available as a routine use to appropriate agencies whether federal, state, local, or foreign, to assist the Department in the evacuation or provision of emergency service to U.S. citizens, or for law enforcement and administration purposes or pursuant to court order. The information is also made available to private U.S. citizens, known as wardens, designated by U.S. embassies to assist in communicating with the American community in an emergency. For a complete statement of the routine uses to which this information may be put, see the Prefatory Statement of Routine Uses and the listing of routine uses set forth in the systems description for Overseas Citizens Services Records (State-05), found at http://foia.state.gov/issuances/priviss.asp. Lastly, while this internet site uses secure encryption to safeguard your privacy and therefore any unauthorized interception by third parties of the information you send via the internet is unlikely, please keep in mind that the Department of State is not responsible for any such interception.

Your Privacy Preferences

☑ I have read the terms of the Privacy Act Notice

● I do not authorize the State Department to disclose my information to anyone except as authorized by law.

○ I agree to allow the State Department to disclose my information to:

☐ Family Members
☐ Friends
☐ Legal Representatives
☐ Media
☐ Medical Representatives
☐ Members of Congress
☐ Other

I

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Access to IBRS/CTF data is restricted to the following:

Department of State OpenNet-based Users

- IBRS administrator;
- Overseas consular users;
- Overseas citizen services domestic users;
- Crisis task force users; and

- Administrative users (Web/System/Database)

<u>Internet-based Users</u>

- Public users (individuals); and
- Organizational users (e.g.,travel agents).

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

At a high level, the following controls are in place establishing criteria, procedures and responsibilities regarding access to CTF and IBRS:

For IBRS administrative users, OCS domestic users and CTF users, a certifying authority is responsible for reviewing each account request and creating the user account. Database administration accounts are reviewed and approved by the CA ISSO andsystem and web administrator accounts are authorized by the Government project manager. Public Internet users access the IBRS Web site anonymously using the ~iusr_IBRS account. After anonymously accessing the IBRS web site, travelers have the option of individually identifying themselves to the web server to register or to change previously entered data.

All levels of access granted to IBRS/CTF users are based on the concepts of least privilege and separation of duties.

A detailed description of the criteria, procedures, controls and responsibilities regarding access is documented in the IBRS System Security Plan (SSP).

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

The IBRS has assigned access authorizations that are enforced in accordance with 12 FAM 629.2-1 and 12 FAM 643.2-1. The following sections describe the level of access/privileges assigned to each IBRS user group.

<u>DoS OpenNet-based Users</u>

IBRS Administrator

The administration (Admin) application of IRBS allows consular users to:

- Maintain travel information functionality which allows consular users to maintain the travel warnings and public announcements issued by the U.S. Department of State to travelers for their posts.
- Maintain Frequently Asked Questions (FAQs) functionality of the Consular Application allows users to modify the content of the homepage of the IBRS website.
- Validating posts functionality of the Admin application allows users to assign one post to validate another's data in IBRS.

Overseas Consular Users

The Consular Application of IBRS allows consular users to manage their posts' data in order to assist U.S. citizens traveling to their post.

From the Consular Application home page, Consular Users can:

- Validate registrants and organizations;
- Reject registrants and organizations;
- Reassign registrants and organizations to another post;
- Register new travelers and organizations;
- Add trips to existing registrations
- Run reports on post data

Overseas Citizen Services Domestic Users

The OCS Domestic Users are comprised of the Washington, DC-based OCS Staff. These users require access to IBRS data for the purposes of oversight and reporting.

Crisis Task Force Users

There are two types of CTF Users: (1) Caseworkers and (2) CTF Admins. Only CTF Admins can set up a crisis in the application and set talking points within the Crisis Manager Tab of CTF. Users who do not have an Admin role assigned to their user account are not presented with the Crisis Manager Tab. This is accomplished in the application through parsing of the login stream in order to determine user ID and the role assigned to the user.

Administrative Users (Web/System/Database)

Database administrators are responsible for the daily maintenance, upgrades, patch/hotfix, and database configuration. The access of database administrators is limited to only those Oracle application files necessary to perform daily activities. This limit of access is controlled through the use of Access Control Lists (ACLs) as established by the system administrators. Although database administrators have privileges that exceed those of a general user, they restrict themselves from using their position to turn off/destroy database audit trails, not to give unauthorized individuals privileged access, and not to modify the system to negate automated security mechanisms.

System administrators have the same security responsibilities of users, but their responsibilities are expanded to recognize their “privileged user” status. They are responsible for daily maintenance, establishing access control lists (ACLs), maintaining user accounts, and backups. Since the duties of system administrators require they be granted full access, the concept of separation of duties is specifically applied. The application of this concept segregates administrators into functional groups such that no single administrator is responsible for the same function (e.g. one administrator will be responsible for system backups while another administrator will handle user account management). System administrators restrict themselves from using their position to turn off/destroy audit trails, not to give unauthorized individuals privileged access, and not to modify the system to negate automated security mechanisms.

<u>Internet-based Users</u>

Public Users (Individuals) and Organizational Users (e.g.,Travel Agents)

The IBRS Internet site allows public users to:

- Sign up for travel warnings, public announcements, and consular information sheets issued by the U.S. Department of State via e-mail for a country of choice; and
- Register trips online.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)

All personnel accessing systems resident on the OpenNet or OpenNet Plus are required to attend the following two security awareness-raising presentations:

1) Diplomatic Security's Security Briefing ; and

2) The Bureau of Consular Affairs in-house Security Awareness presentation.

Both presentations require signed acknowledgement of the rules of behavior and include segments covering appropriate system usage and formal statements on the Rules of Behavior regarding DoS computer systems.

Internet users who access IBRS via the travel.state.gov website are presented with Privacy and Computer Fraud and Abuse Act Notices describing their expected behavior while accessing the IBRS web site. Additionally, since the public user's registration is used to make their presence and whereabouts known in the event of an emergency, it is expected that these users would not want to misuse their own data.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Yes. Contractors are involved with the design and development of the IBRS/CTF system and will be involved with the maintenance of the system. Privacy Act information clauses have been inserted into all Statements of Work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings covering the handling of classified and other such information prior to working on the task.

6) Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

7) IBRS data is only available from CCD and ACS; both systems are owned by the Bureau of Consular Affairs (CA) and, therefore, the same protections are in place for CCD and ACS as IBRS.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?

No agencies external to CA have access to the data in IBRS and CTF.

9) Who is responsible for assuring proper use of the SHARED data?

The CA/CST system owner is responsible for the proper handling of data that is shared between information systems within CA.