PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Impact Assessment

Is this a new or substantially revised electronic information system? If revised, describe revisions.

The Crime Incident Reporting System (CIRS) application is a substantially revised electronic information system from the original MS-excel-based Crime Incident Reporting Form (CIRF).

From a technology standpoint, the CIRS application is designed and developed as a component of the Aquifer Web Application Services Framework (Aquifer). Aquifer is a General Support System (GSS) that provides a hosting environment for fully complied, .NET application components. The CIRS application is based on the Aquifer 3-tier architecture and has four distinct components for CIRS specific functionality.

· CIRS Client Interface (Peace Corps desktop and laptop user interface)

· CIRS Remote Access Interface (External PDA/Blackberry user interface)

· CIRS Server-side Web Service (Business process management and client communications)

· CIRS Database (Data management)

From the standpoint of the users, the CIRS application provides posts with an internet-accessible crime incident report system that allows appropriate staff at Headquarters (HQ) and Post to input, update, query and retrieve data from a centralized database. It provides for protection of the Volunteer identifying information and maintains the confidentiality of that information through encrypted communications, role-based access to the data and unique user i.d.s and passwords access management. With a centralized repository of information, problems, which had occurred under CIRF with data inconsistency, are reduced. The system provides generic e-mail alerts to notify staff at HQ and at Post that a new incident has occurred. The system also auto-sends emails when updates/changes to existing incidents have been made to critical fields. The email notifications are designed to occur immediately after an incident is submitted to HQ, whereas with the CIRF, email notifications were manually sent by the reporting individual.

If any question does not apply, state not applicable (N/A) for each question and explain why.

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

Records compiled by Crime Incident Reporting (CIRS) users at post (e.g., Country Directors, Safety and Security Coordinators, Peace Corps Medical Officers, etc.) and headquarters (e.g., Office of Safety and Security and Regions) consist of personal data on Volunteers who are victims. The data includes Volunteer name; contact information; Volunteer address if incident occurred at the Volunteer's home in the Volunteer's country of service; Volunteer tag (system-generated ID associated with the Volunteer's name); race; ethnicity; sex; marital status; age; length of time in service when incident occurred; sector; country of incident, country of service; date of incident; date incident was reported to post; time of incident; date of incident; personnel notified; population of community (i.e., urban, intermediate, or rural); incident location; site information; nature and details of the incident/offense, including whether alcohol, drugs and/or weapons were involved; type of injury; medical/counseling support provided/planned; whether an alleged offender was apprehended; and victim's intention to prosecute; and follow up information on the case.

Records also include information taken about alleged offenders and witnesses, who could be citizens of the host country or U.S. staff or Volunteers. Data on alleged offenders include name; sex; age; relationship of alleged offender to victim; whether alleged offender used alcohol; and a text field for additional alleged offender information, such as tattoos, scars, etc. Witness data includes name; contact information; and a text for additional witness information.

II. Why is the information being collected (e.g., to determine eligibility)?

The system notifies in a timely manner Peace Corps headquarters and overseas staff who have a need to know when a crime has occurred against a Volunteer. Such staff make safety and security, medical, or management decisions regarding the Volunteer victim. The system also notifies the U.S. Embassy's Regional Security Officers covering the post whenever a crime against a Volunteer has occurred.

Finally, the database provides a single central facility within the Peace Corps to record crime incidents against Volunteers and to provide statistical information, without personal identifiers, to interested public and internal audiences.

III. How will the information be used (e.g., to verify existing data)?

The data will be used to notify the Volunteer Security and Overseas Support division of the Office of Safety and Security, as well as other Peace Corps staff with a need to know, when a crime occurs that would require investigative support for the Volunteer. The system also notifies the U.S. Embassy's Regional Security Officers covering the post whenever a crime against a Volunteer occurs so that they may initiate investigative procedures, as necessary. The data will be used for statistical purposes to enhance Peace Corps' ability to track crimes against Volunteers, analyze trends and to respond to executive, legislative, and oversight requests for statistical crime data. The Peace Corps also uses this information for programmatic and training purposes, to evaluate the circumstances of crimes against Peace Corps Volunteers, and to make any necessary changes in policy and/or programs.

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

The number of incidents, as well as Volunteer victim and alleged offender characteristics, are analyzed and compiled into several sources, including the annual Safety of the Volunteer (SOV) report, incident frequency reports, and ad-hoc data requests from internal and external persons requesting data on the nature of safety incidents concerning Volunteers. A pdf version of the SOV report is available on the external Peace Corps website and the internal Intranet. When requested, a copy is provided to members of Congress. Regional Security Officers and Assistant Regional Security Officers, who are Department of State employees, are also provided crime incident information for investigative purposes. With the exception of reports provided to the Department of State security officers, these reports do not include personally identifiable information.

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

Effectively, Volunteers who are reporting an incident are not offered an opportunity to decline to provide information about the crime or to consent to particular use of the information.

VI. How will the information be secured (e.g., administrative and technological controls)?

Participant information will only accessible by a designated system administrator and only through the use of a system administrator's password. Information will be encrypted using 128-bit SSL and AES encryptions standards. Through coordination with the Office of the Chief Information Officer, the CIRS system platform completed the accreditation process with the WebTrust seal as well as a SAS-70 Type II audit, which was performed by a third party auditor. On February 2008, the CIRS application was accredited and granted full Authority to Operate.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)? Will a System of Record Notice be created under the Privacy Act, 5 U.S.C. 552a?

The data can be retrieved using any of the CIRS data fields. These include Volunteer Tag (system-generated ID associated with the Volunteer's name); race/ethnicity; sex; country of incident, country of service; sector of assignment; marital status; age; Volunteer site; type of incident; date of incident; date incident was reported to post; time of incident; personnel notified; incident location; size of population of community (i.e., urban, intermediate, rural); nature and details of the incident; alcohol use by Volunteer at time of incident; weapon use by alleged offender; injury sustained; medical/counseling support provided; victim's intention to prosecute; and alleged offender's motive for committing incident; name of alleged offender; age range of alleged offender; gender of alleged offender; relationship of alleged offender to victim; alcohol use by alleged offender at time of incident; whether alleged offender was apprehended; information on witnesses, and post follow up or changes to original incident report, as noted in the updates section of the incident report.

Volunteer name; Volunteer contact information, including phone number, address, and/or email address are housed in the database but are only seen by a limited audience. These fields are not readily retrievable through any searching mechanisms built into CIRS nor are they pulled by the Crime Statistics and Analysis Unit during normal data retrieval processes.

A System of Records Notice PC - **33** was created for this system.