Privacy Impact Assessment: Office of Inspector General Case Management System

Version 1.0

December 3, 2003

Office of the Privacy Advocate IS: PA
United States Peace Corps
1111 20th St. NW
Washington, DC 20652

TABLE OF CONTENTS

SECTION I
INTRODUCTION AND OVERVIEW

Introduction

The United States Peace Corps recognizes the importance of protecting the privacy of volunteers, returned volunteers (further referred to as volunteers), and employees, especially as it modernizes its volunteer and employee systems. Privacy issues must be addressed when systems are being developed, and privacy protections must be integrated into the development life cycle of these automated systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA). The PIA process also provides a means to assure compliance with applicable laws and regulations governing volunteer and employee privacy.

Purpose

The purpose of this document is to:

- Establish the requirements for addressing privacy during the systems development process;
- Describe the steps required to complete a PIA on a project;
- Define the privacy issues a project must address when completing a PIA.

Background

The United States Peace Corps is responsible for ensuring the privacy, confidentiality, integrity, and availability of volunteer and employee information. The Peace Corps recognizes that privacy protection is both a personal and fundamental right of all volunteers and employees. Among the most basic of volunteers and employees rights is an expectation that the Peace Corps will protect the confidentiality of personal, financial, and employment information. Volunteers and employees also have the right to expect that the Peace Corps will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities. Volunteer and employee information is protected by the following:

- Privacy Act of 1974, as Amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503);
- Computer Security Act of 1987 (Public Law 100-235) which establishes minimum security practices for Federal computer systems;
- OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems;
- Freedom of Information Act, as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

Office of the Privacy Advocate

The Office of the Privacy Advocate is the Peace Corps organization responsible for overseeing volunteer and employee privacy. The Office was established in January 1993 under the Chief Information Officer. The mission of the Office of the Privacy Advocate is to formulate, develop, implement, and promote effective volunteer and employee privacy protection strategies and programs. These strategies and programs will enhance the efforts of the Peace Corps to earn the highest degree of public confidence in its integrity, efficiency, and fairness. The Office of the Privacy Advocate developed the Privacy Principles, which were disseminated by the Commissioner in May 1994. Policy Statement P-1-1, Volunteer Privacy Rights was signed by the Commissioner in October 1994. The Privacy Principles are in Appendix A and the Policy Statement is in Appendix B of this document.

SECTION II

PRIVACY IMPACT ASSESSMENT

Privacy and Systems Development

Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. The Office of the Privacy Advocate has instituted the Privacy Impact Assessment in order to ensure that the systems the Peace Corps develops protect individuals privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

What is a Privacy Impact Assessment?

The Privacy Impact Assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Privacy Advocate. The PIA process is described in detail in Section III, Completing a Privacy Impact Assessment.

When is a PIA done?

The PIA is to be initiated in the early stages of the development of a system and completed as part of the required SLC reviews.

Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in the Peace Corps.

Who completes the PIA?

Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

What systems have to complete PIA?

New systems, systems under development, or systems undergoing major modifications are required to complete a PIA. The Privacy Advocate does reserve the right to request that a PIA be completed on any system that may have privacy risks. More specifically:

- New systems and systems under development or undergoing major modifications are required to complete a PIA.
- Legacy systems, as they exist today, do not have to complete a PIA. However, if the automation or upgrading of these systems puts the data at risk, a PIA may be requested by the Privacy Advocate.
- Currently operational systems are not required to complete a PIA. However, if privacy is a concern for a system the Privacy Advocate can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the Peace Corps will use best, or all reasonable, efforts to remedy the problem.

SECTION III
COMPLETING A PRIVACY IMPACT ASSESSMENT

The PIA

This section describes the steps that are required to complete a PIA. These steps are summarized in Table 1, Outline of Steps for Completing a PIA.

Training

Training on the PIA will be available, upon request, from the Office of the Privacy Advocate. The training describes the PIA process and provides detail about the privacy issues and privacy questions to be answered to complete the PIA. The intended audience is the personnel responsible for writing the PIA document. PIA training is available to government and contractor personnel.

The PIA Document

Preparing the PIA document requires the system owner and developer to answer the privacy questions in Section V. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as Not Applicable. During the development of the PIA document, the Office of the Privacy Advocate will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.

Review of the PIA Document

The completed PIA document is to be submitted to the Office of the Privacy Advocate for review. The purpose of the review is to identify privacy risks in the system. The Office of the Privacy Advocate will work with the system owner and system developer to develop design requirements to resolve the identified risks. If there are risks in a system that cannot be resolved with the Privacy Advocate, the risks will be presented to the CIO for resolution.

Approval of the PIA

The SLC review process will be used to validate the incorporation of the design requirements to resolve the privacy risks. Formal approval will be issued in accordance with the SLC.

Table 1

Outline of Steps for Completing a PIA

Step	Who	Procedure
1	System Owner, and Developer	Request and complete Privacy Impact Assessment (PIA) Training.
2	System Owner, and Developer	Answer the questions in Section V Privacy Questions.
3	System Owner,	Submit the PIA document to the Privacy Advocate.

	and Developer	
4	Office of the Privacy Advocate (PA)	Review the PIA document to identify privacy risks from the information provided. The Privacy Advocate will get clarification from the owner and developer as needed.
5	System Owner, Developer, PA, and CIO	The System Owner, Developer and the Privacy Advocate should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached then issues will be raised to the CIO for resolution.
6	System Owner, and Developer	The System Owner and Developer will incorporate the agreed upon design requirements and resolve the identified risks.
7	System Owner, Developer, and PA	Participate in the SLC required reviews to ensure satisfactory resolution of identified privacy risks and obtain formal approval.

SECTION IV
PRIVACY ISSUES IN INFORMATION SYSTEMS

Privacy Act of 1974 5 U.S.C. 552a As Amended

The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically:

"each agency that maintains a system of records shall -"

- "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;"

- "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individuals rights, benefits, and privileges under Federal programs;"

- "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;"

- "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Definitions:

Accuracy - within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness - all elements necessary for making a determination are present before such determination is made.

***Determination* -** any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Necessary - a threshold of need for an element of information greater than mere relevance and utility.

***Record* -** any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance - limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

Routine Use - with respect to the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected.

System of Records - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Information and Privacy

To fulfill the commitment of the Peace Corps to protect volunteer data several issues must be addressed with respect to privacy.

- The use of information must be controlled.
- Information may be used only for a necessary and lawful purpose.
- Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
- Information collected for a particular purpose should not be used for another purpose without the data subjects consent unless such other uses are specifically authorized or mandated by law.
- Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the Peace Corps, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the Peace Corps to the laws which protect volunteer and employee privacy rights and which provide redress for violations of those rights.

Data in the System

The sources of the information in the system are an important privacy consideration if the data is gathered from other than Peace Corps records. Information collected from non-Peace Corps sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. This is especially important if the information will be used to make determinations about individuals.

Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, state, or local entities that have access to Peace Corps data.

Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be *relevant* and *necessary* to accomplish the purpose of the system. Second, the data must be *complete, accurate* and *timel*y. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory and/or IRM requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly eliminated at the end of that time.

The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of volunteers and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some judicially ascertainable standard of reasonableness in light of the statutory mission of the Peace Corps and other authorized governmental users of the system.

SECTION V

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.

Peace Corps entelliTrak IG-CMS will be used for the management of inquiries and cases that are investigated by the Office of Inspector General (OIG). Data will be captured when applicable for the following types of individuals in the capacities listed below:

- Employee – The OIG receives complaints and allegations about employees, both domestically and abroad. Data pertaining to such allegations are collected and analyzed to confirm or refute charges. In effort to ferret out fraud, waste, and abuse, any Peace Corps' employees may be investigated by the OIG. The types of information collected during an investigation are dependent upon the allegations or complaints raised. Electronic mail, personnel files, time and attendance records, vouchers, or other documents may be gathered. The OIG will enter case related materials in the entelliTrak IG-CMS. Such data will include: employee name, age, gender, address, phone number, date of birth, criminal history, sentences, fines, restitution, explanation or observation of events, victims, witness information etc. In the event of a Peace Corps employee being involved as the subject, victim, witness or point of contact in an investigation, such data would be captured as part of the electronic case record. In the event of a claim filed as a result of said employee sustaining a work-related injury, FECA Claim information may be tracked to include the following items as needed: Name, Unique ID, Claimant Number, Location, Pre-existing Condition (if any), Injury/Illness, and Compensation Information.
- Volunteer – In the event that a Peace Corps Volunteer is involved in an Inquiry or Full Investigation as a Victim, Subject or other contact, the information captured where pertinent and available may include: Name, Age, Gender, Address, Phone, Email, Unique ID, DOB, Criminal History, and Sentence/Fine/Restitution for case Subjects if applicable. In the event of a claim filed by the Volunteer for an injury or illness related to their Volunteer Activities, FECA Claim information may be tracked to include the following items as needed:

Name, Unique ID, Claimant Number, Location, Pre-existing Condition (if any), Injury/Illness, and Compensation Information.

- Other - Other individuals involved with a given Inquiry or Investigation as a Subject, Victim, or other contact may include the following if pertinent: Name, Age, Gender, Address, Phone, Email, Unique ID, DOB, Criminal History, and Sentence/Fine/Restitution for case Subjects if applicable.
- Other general case related data available in the system may include statistical reports and / or general case descriptions and activities performed in the course of the investigation. Specific data captured and methods of documentation are dictated by internal OIG policy. For detailed information regarding data captured within entelliTrak IG-CMS by table and field and descriptions of the exact nature of said data, please see *Appendix MPE-A – Peace Corps entelliTrak IG-CMS Data Dictionary.*

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?

Sources of information tracked by this system are variable and subject to the type of Inquiry or Investigation being recorded. Files originating from Peace Corps that are attached to the electronic case record may include (but are not limited to): Reports on Investigation Activities, Evidence Documents, Prosecution Reports and Memos. Federal, State, Local Agencies and third-party sources from which data is collected will greatly depend upon the needs of the Inquiry or Investigation. Information collected from volunteers and/or employees will vary by individual and said individual's level of involvement, but may include the following at a high level: General Inquiry such as Date and Location of Incident, Victim, Subject and Other Contact information, Investigative Plan details, Memoranda of Activities, FECA Claims, Evidence Information, Administrative Events, Subpoenas, and overall Case Disposition. For more information regarding data tracked within entelliTrak IG-CMS please see *Page 10, Question 1* and *Appendix MPE-A – Peace Corps entelliTrak IG-CMS Data Dictionary.*

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?

Methods of collecting and verifying data are varied by objections of the investigation. Title 18: USC Criminal Codes outlines many of the kind of investigations performed by the OIG. Data is collected through oral testimony, subpoenas, surveillances, physical records, etc. Factors pertaining to verifying the accuracy and completeness of Inquiry and/or Case related information may include (but would not be limited to) authority, ability to corroborate, plausibility, and presentation of said information. Data tracked within the entelliTrak IG-CMS application will be recorded with date of entry, method of collection, source, etc.

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

All data elements captured in the Peace Corps entelliTrak IG-CMS are listed in the entelliTrak data dictionary. See *Appendix MPE- A – Peace Corps entelliTrak IG-CMS Data Dictionary*.

Access to the Data

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

Access to the system data will primarily be limited to Agents (Users), Managers, and Administrators within the OIG. Technical support will be provided on behalf of Peace Corps by project staff from MicroPact Engineering, Inc. however these individuals will not have standard login access to the Application's User Interface. For specific and detailed information pertaining to user/login access by role, please see *Appendix MPE-B – Role/Tab Access (OIG Tracking System Tab Access Privileges by Role).*

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

All application-level access is managed by the Agency (Peace Corps OIG) in order to preserve the Agency's approved processes. User account requests will be sent via email to the designated Admin appointed by Peace Corps OIG, who will grant access after verifying that the requestor's official duties necessitate access to the application. The Computer Security Coordinator will provide training on application use and procedures prior to granting access.

New hires in the office of Inspector General are entered into the Personnel Tracking System (which confirms the new hire's receipt and signing of the

Technical Access Agreement). The System Owner or Computer Security Coordinator are responsible for verifying the appropriate BI is complete and that the person's job duties make it necessary to grant user access to the entelliTrak IG-CMS system. Upon doing so an email request would be sent including the user's required role (level of access). Multiple roles can be assigned. For specific and detailed information pertaining to user/login access by role, please see *Appendix MPE- B – Role/Tab Access (OIG Tracking System Tab Access Privileges by Role).*

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

Access to data is restricted by role based upon the needs of the user as it pertains to their job function. User roles may restrict them from entire pages of data or from the ability to edit and delete data. For example, most standard user roles will not have access to Administrator functionality such as account management information. See *Appendix MPE-B – Role/Tab Access (OIG Tracking System Tab Access Privileges by Role)* for details regarding the access that each user role within the entelliTrak IG-CMS Application will have.

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

As described in *Page 12, Questions 2 and 3*, access to data is restricted by role based upon the needs of the user as it pertains to their job function. Appropriate use of available data would largely be dictated by policy internal to the Peace Corps OIG. Activity and Audit logs are available within the application to further aid in spotting potential system misuse. As needed user roles and access can be further restricted, and in addition user accounts can be temporarily locked or permanently disabled as needed by either the System Owner or the CSC.

5. a. Do other systems share data or have access to data in this system? If yes, explain.
b. Who will be responsible for protecting the privacy rights of the volunteers and employees affected by the interface?

There is no interconnectivity or data sharing that occurs between the entelliTrak IG-CMS application and any other Peace Corps or non-Peace Corps system and as such this question is non-applicable.

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

b. How will the data be used by the agency?
c. Who is responsible for assuring proper use of the data?

As a matter of standard policy no other agencies will have login access to the data in the entelliTrak IG. Data tracked in the entelliTrak IG-CMS system should be for use by Peace Corps OIG employees only and used primarily for the automated tracking of Inquiries and Investigations, to aid in the automation of Federally-mandated reporting, etc. Proper use of the Application will be overseen by the System Owner and the CSC.

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?

Requirements gathering sessions have been held prior to system implementation as a collaborative effort between the System Owner, CSC, System Developers, and OIG End-users in order to ensure that the data being captured within entelliTrak IG-CMS is both relevant and necessary for its intended purpose. Data fields deemed no longer necessary can be permanently removed at the request of the System Owner or CSC as needed.

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?

The entelliTrak IG-CMS Application will not derive new data or create otherwise unavailable data through aggregation about any individual and as such this question is not applicable.

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.

Data within the entelliTrak IG-CMS Application will not be consolidated or linked with any other system. Data is only accessed by authorized users over a secure connection with the use of Secured Certificates to verify the identity of the user accessing the system.

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?

Data within the entelliTrak IG-CMS Application can be retrieved by authorized users only, through the use of searching and to a limited degree reporting. Records can be searched by all data-entry elements tracked within the system including personal identifiers such as name and Unique ID if said information has been entered. The ability to search for specific data elements can be restricted through configuration settings if deemed necessary at the request of the System Owner and CSC. Potential effects on due process are dependant upon the type of Inquiry or Investigation being tracked, and the individual(s) involved. Consolidation and linkage of files and systems, and derivation of data about and individual will not apply to this system.

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.

While the system will be accessible by authorized users from multiple locations, the database on which the applicable data is stored will be housed in a central location for ease and consistency of maintenance, and the application will only be accessed by the user's Peace Corps-issued computer. Access will be limited to individuals with appropriate Peace Corps-specific agent training who will be well-schooled in the appropriate treatment of individuals involved with an Inquiry or Investigation as a result of that training.

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?

Peace Corps OIG initial timeframe for maintaining electronic records (via excel spread sheet) began in 1998. Retention periods within this system will be determined by internal Peace Corps OIG policy for electronic record and archive retention. Data can be deleted or archived as deemed necessary by the System Owner or CSC. Accuracy, relevance, and timeliness of data can be determined through means such as periodic case reviews and can be deleted or otherwise removed from the system if deemed no longer necessary.

3. a. Is the system using technologies in ways that the Peace Corps has not previously employed (e.g. Caller-ID)?
b. How does the use of this technology affect volunteer/employee privacy?

The entelliTrak IG-CMS does not employ any technologies that have not been previously employed by Peace Corps.

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?

The capability to locate and identify individuals will be limited to personally identifiable information (PII) such as Name, Address, Phone Number, and Unique IDs. Monitoring of individuals is not performed through this system. The capability to identify, locate, and monitor groups of people does not exist in this system per se.

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..

The Peace Corps is subject to the Health Insurance Portability and Accountability Act (HIPAA). Modifications to the system configuration should not require any amendments to the SOR. For more information, please refer to the *Peace Corps Notice of Privacy Practices* located at http://www.peacecorps.gov/policies/pdf/hipaa.pdf, and *Appendices A and B of this document.*

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Peace Corps to the volunteers and are the responsibility of all Peace Corps employees to recognize and treat their office as a public trust.

The obligation to protect volunteer privacy and to safeguard the information volunteers entrust to us is a fundamental part of the Peace Corps mission. Volunteers have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of volunteers personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of Peace Corps data systems, processes and facilities.

All Peace Corps employees are required to exhibit individual performance that reflects a commitment to dealing with every volunteer fairly and honestly and to respect the volunteers right to feel secure that their personal information is protected. To promote and maintain volunteers' confidence in the privacy, confidentiality and security protections provided by the Peace Corps, the Peace Corps will be guided by the following Privacy Principles:

Principle 1: Protecting volunteer privacy and safeguarding confidential volunteer information is a public trust.

Principle 2: No information will be collected or used with respect to volunteers that is not necessary and relevant for legally mandated or authorized purposes.

Principle 3: Information will be collected, to the greatest extent practicable, directly from the volunteer to whom it relates.

Principle 4: Information about volunteers collected from third parties will be verified to the greatest extent practicable with the volunteers themselves before action is taken against them.

Principle 5: Personally identifiable volunteer information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.

Principle 6: Personally identifiable volunteer information will be disposed of at the end of the retention period required by law or regulation.

Principle 7: Volunteer information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the Peace Corps other than as authorized by law and in the performance of official duties.

Principle 8: Browsing, or any unauthorized access of volunteer information by any Peace Corps employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.

Principle 9: Requirements governing the accuracy, reliability, completeness, and timeliness of volunteer information will be such as to ensure fair treatment of all volunteers.

Principle 10: The privacy rights of volunteers will be respected at all times and every volunteer will be treated honestly, fairly, and respectfully. The Declaration does not, in itself, create any legal rights for volunteers, but it is intended to express the full and sincere commitment of the Peace Corps and its employees to the laws which protect volunteer privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON VOLUNTEER PRIVACY RIGHTS

The Peace Corps is fully committed to protecting the privacy rights of all volunteers. Many of these rights are stated in law. However, the Peace Corps recognizes that compliance with legal requirements alone is not enough. The Peace Corps also recognizes its social responsibility which is
implicit in the ethical relationship between the Peace Corps and the volunteer. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a volunteer's privacy rights is an expectation that the Peace Corps will keep personal and financial information confidential. Volunteers also have the right to expect that the Peace Corps will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The Peace Corps will safeguard the integrity and availability of volunteers personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all volunteers. Peace Corps employees will perform their duties in a manner that will recognize and enhance individuals rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the Peace Corps will respect the individuals exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the Peace Corps takes very seriously its social responsibility to volunteers to limit and control information usage as well as to protect public and official access. In light of this responsibility, the Peace Corps is equally concerned with the ethical treatment of volunteers as well as their legal and administrative rights.

APPENDIX MPE-A
PEACE CORPS entelliTrak IG-CMS DATA DICTIONARY

Appendix A - Peace Corps entelliTrak IG-CMS Data Dictionary

Activity Type (T_ACTIVITY_TYPE)

Activity Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Address Type (T_ADDRESS_TYPE)

Address Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Admin Event Type (T_ADMIN_EVENT_TYPE)

Admin Event Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name
Role Filter	C_ROLE_FILTER	Text	Role Filter
Special Filter	C_SPECIAL_FILTER	Text	Special Filter
State Filter	C_STATE_FILTER	Text	State Filter

Agent Type (T_AGENT_TYPE)

Agent Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name
User ID	C_USER_ID	Text	User ID

Allegation Type (T_ALLEGATION_TYPE)

Allegation Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Alphabet Type (T_ALPHABET_TYPE)

Alphabet Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Contact Status Type (T_CONTACT_STATUS_TYPE)

Contact Status Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Disposition Type (T_DISPOSITION_TYPE)

Disposition Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name
State Filter	C_STATE_FILTER	Text	State Filter

District Type (T_DISTRICT_TYPE)

District Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Document Type (T_DOCUMENT_TYPE)

Document Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Evidence Disposition Type (T_EVIDENCE_DISPOSITION_TYPE)

Evidence disposition - returned, destroyed, etc

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	ETP Code if needed.

Evidence disposition - returned, destroyed, etc

Element Name	Column Name	Data Type	Description
Name	C_NAME	Text	Name of Evidence Disposition

Gender Type (T_GENDER_TYPE)

Gender Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Investigation Status Type (T_INVESTIGATION_STATUS_TYPE)

Investigation Status Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Investigation Type (T_INVESTIGATION_TYPE)

Investigation Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Allegation Type Filter	C_ALLEGATION_TYPE_FILTER	Text	Allegation Type Filter
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Location Type (T_LOCATION_TYPE)

Location Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name
Region Filter	C_REGION_FILTER	Text	Region Filter

Memo_ref (T_MEMO_REF)

Reference table for Memorandum report

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Analysis & Conclusions	C_ANALYSIS__CONCLUSIONS	Text	Analysis & Conclusions
Background	C_BACKROUND	Text	Background
Facts	C_FACTS	Text	Facts
Recommendations	C_RECOMENDATIONS	Text	Recommendations
Special Agent	C_SPECIAL_AGENT	Text	Special Agent

MOA Activity Type (T_MOA_ACTIVITY_TYPE)

MOA Activity Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Nationality Type (T_NATIONALITY_TYPE)

Nationality Type defines whether the person in question is a host country national or an American citizen.

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	ETP Code if needed
Name	C_NAME	Text	Name of Nationality Type

Plan Type (T_PLAN_TYPE)

Plan Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Post Type (T_POST_TYPE)

Post Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name
Region Filter	C_REGION_FILTER	Text	Region Filter

Refer to USDOJ Type (T_REFER_TO_USDOJ_TYPE)

Refer to USDOJ Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Referred to Peace Corps Type (T_REFFERED_TO_PEACE_CORPS_TYPE)

Referred to Peace Corps Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Region Type (T_REGION_TYPE)

Region Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Source of Contact Type (T_SOURCE_OF_CONTACT_TYPE)

Source of Contact Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Nam

State Type (T_STATE_TYPE)

State Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Subject Disposition Type (T_SUBJECT_DISPOSITION_TYPE)

Subject Disposition Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Subject Type (T_SUBJECT_TYPE)

Subject Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Suffix Type (T_SUFFIX_TYPE)

Suffix Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Title Type (T_TITLE_TYPE)

Title type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Name	C_NAME	Text	Name

Tracking Sequence (T_TRACKING_SEQUENCE)

Tracking Sequence

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Date Column	C_DATE_COLUMN	Text	Date Column
Prefix	C_PREFIX	Text	Prefix
Table Name	C_TABLE_NAME	Text	Table Name
Value	C_VALUE	Number	Value

Violation Type (T_VIOLATION_TYPE)

Violation category - Title 18, violent crime, etc.

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	ETP Code if necessary.
Name	C_NAME	Text	Name of violation category.

Weapon Type (T_WEAPON_TYPE)

Specific type of weapon used in alleged incident.

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	ETP Code, if needed.
Name	C_NAME	Text	Name of weapon type.

YesNo Type (T_YESNO_TYPE)

YesNo Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

YesNoNa Type (T_YESNONA_TYPE)

YesNoNa Type

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Code	C_CODE	Text	Code
Name	C_NAME	Text	Name

Inquiry (T_INQUIRY)

Inquiry

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
Agent	C_AGENT	Number	Agent
CIRF Number	C_CIRF_NUMBER	Text	Cross-reference number for violent crimes.
Date Occured	C_DATE_OCCURED	Date	Date Occured
Disposition	C_DISPOSITION	Number	Disposition
Injury	C_INJURY	Text	Injury
Inquiry Number	C_INQUIRY_NUMBER	Text	Preliminary inquiry ID #.
Inquiry Open Date	C_INQUIRY_OPEN_DATE	Date	Inquiry Open Date
Investigation Number	C_INVESTIGATION_NUMBER	Text	Investigation number is automatically generated when the inquiry becomes a case.
Investigation Type	C_INVESTIGATION_TYPE	Number	Investigation Type
Location	C_LOCATION	Number	Location
Location of Incident	C_LOCATION_OF_INCIDENT	Text	Location of Incident
Narrative	C_NARRATIVE	Text	Narrative
Notification	C_NOTIFICATION	Text	Notification
Region	C_REGION	Number	Region
Source of Contact	C_SOURCE_OF_CONTACT	Number	Source of Contact
State	ID_WORKFLOW	State	Workflow Business Process State
Subpoena	C_SUBPOENA	Number	Subpoena
Weapon	C_WEAPON	Number	Weapon
Weapon Type	C_WEAPON_TYPE	Number	Specific type of weapon used in alleged incident.

Victim (T_VICTIM)

Victim

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Age	C_AGE	Number	Victim's age - calculated from DOB.
AKA	C_AKA	Text	AKA
Cell Phone	C_CELL_PHONE	Text	Cell Phone
Comments	C_COMMENTS	Text	Comments
Criminal History	C_CRIMINAL_HISTORY	Text	Victim's criminal history, if any
DOB	C_DOB	Date	Victim's date of birth.
Drivers License Number	C_DRIVERS_LICENSE_NUMBER	Text	Drivers license # if different from SSN
Email	C_EMAIL	Text	Email
First Name	C_FIRST_NAME	Text	First Name
Gender	C_GENDER	Number	Gender
Home Phone	C_HOME_PHONE	Text	Home Phone
Job Title	C_JOB_TITLE	Text	Victim's job title / position.
Last Name	C_LAST_NAME	Text	Last Name
Middle Name	C_MIDDLE_NAME	Text	Middle Name
Nationality	C_NATIONALITY	Number	Defines whether the individual is a Host Country National or American Citizen.
SSN	C_SSN	Text	SSN
Suffix	C_SUFFIX	Number	Suffix
VIDA Number	C_VIDA_NUMBER	Text	Peace Corps-specific volunteer identifier.
Work Phone	C_WORK_PHONE	Text	Work Phone

Subject (T_SUBJECT)

Subject

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Age	C_AGE	Number	Subject's age - calculated from DOB.
AKA	C_AKA	Text	AKA
Cell Phone	C_CELL_PHONE	Text	Cell Phone
Comments	C_COMMENTS	Text	Comments
Criminal History	C_CRIMINAL_HISTORY	Text	Subject's prior criminal history, if any.
DOB	C_DOB	Date	Subject's date of birth.
Drivers License Number	C_DRIVERS_LICENSE_NUMBER	Text	Number on driver's license if different from SSN.
Email	C_EMAIL	Text	Email
First Name	C_FIRST_NAME	Text	First Name
Gender	C_GENDER	Number	Gender
Home Phone	C_HOME_PHONE	Text	Home Phone
Job Title	C_JOB_TITLE	Text	Subject's job title/position.
Last Name	C_LAST_NAME	Text	Last Name
Middle Name	C_MIDDLE_NAME	Text	Middle Name
Nationality	C_NATIONALITY	Number	Defines whether the individual is a Host Country National or American Citizen.

Subject

Element Name	Column Name	Data Type	Description
SSN	C_SSN	Text	SSN
Subject Type	C_SUBJECT_TYPE	Number	Subject Type
Suffix	C_SUFFIX	Number	Suffix
VIDA Number	C_VIDA_NUMBER	Text	Peace Corps specific unique volunteer id.
Work Phone	C_WORK_PHONE	Text	Work Phone

Contacts (T_CONTACTS)

Contacts

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Age	C_AGE	Number	Age of contact - calculated from DOB.
AKA	C_AKA	Text	AKA
Cell Phone	C_CELL_PHONE	Text	Cell Phone
Comments	C_COMMENTS	Text	Comments
Contact Status	C_CONTACT_STATUS	Text	Contact Status
DOB	C_DOB	Date	Contact's date of birth.
Drivers License Number	C_DRIVERS_LICENSE_NUMBER	Text	Number on driver’s license if different from

Contacts

Element Name	Column Name	Data Type	Description
			SSN.
Email	C_EMAIL	Text	Email
First Name	C_FIRST_NAME	Text	First Name
Gender	C_GENDER	Number	Gender
Home Phone	C_HOME_PHONE	Text	Home Phone
Job Title	C_JOB_TITLE	Text	Contact's job title/position.
Knowledge of Investigation	C_KNOWLEDGE_OF_INVESTIGATION	Text	Information provided by the individual about the investigation.
Last Name	C_LAST_NAME	Text	Last Name
Middle Name	C_MIDDLE_NAME	Text	Middle Name
Nationality	C_NATIONALITY	Number	Defines whether the individual is a Host Country National or American Citizen
SSN/ID	C_SSNID	Text	SSN/ID
Suffix	C_SUFFIX	Number	Suffix
VIDA Number	C_VIDA_NUMBER	Text	Peace Corps specific unique volunteer identifier.
Work Phone	C_WORK_PHONE	Text	Work Phone

Investigative Plan (T_INVESTIGATIVE_PLAN)

Investigative Plan

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference

Investigative Plan

Element Name	Column Name	Data Type	Description
			to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Allegation Type	C_ALLEGATION_TYPE	Number	Allegation Type
Allegations	C_ALLEGATIONS	Text	Allegations
Case In Progress Date	C_CASE_IN_PROGRESS_DATE	Date	Case In Progress Date
Comments	C_COMMENTS	Text	Comments on the IP either from the AIGI or Agent.
Convert to Full	C_CONVERT_TO_FULL	Yes/No	Convert to Full
Investigation Number	C_INVESTIGATION_NUMBER	Text	Investigation number is automatically generated when the inquiry becomes a case.
Investigator	C_INVESTIGATOR	Number	Investigator
Plan Date	C_PLAN_DATE	Date	Plan Date
Plan Type	C_PLAN_TYPE	Number	Plan Type
Planned Activities	C_PLANNED_ACTIVITIES	Text	Planned Activities
Signature	C_SIGNATURE	Password	Signature

MOA/ MOI (T_MOA_MOI)

MOA/ MOI

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry

MOA/ MOI

Element Name	Column Name	Data Type	Description
			(T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Activity Date	C_ACTIVITY_DATE	Date	Activity Date
Activity Time	C_ACTIVITY_TIME	Text	Activity Time
Activity Type	C_ACTIVITY_TYPE	Number	Activity Type
Agent	C_AGENT	Number	Agent
Details	C_DETAILS	Long Text	Details
Investigation Number	C_INVESTIGATION_NUMBER	Text	Investigation Number that was generated upon case creation.
Location	C_LOCATION	Text	Location
MOA Upload	C_MOA_UPLOAD	File	Document upload field to allow uploading of an MOA document rather than typing directly into the user interface.
Reviewed By	C_REVIEWED_BY	Password	Reviewed By

ROI (T_ROI)

ROI

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key

ROI

Element Name	Column Name	Data Type	Description
			reference to the base tracking object ID.
Approval Signature	C_APPROVAL_SIGNATURE	Password	Supervisory Approval Signature
Date	C_DATE	Date	Data Entry Date
Details	C_DETAILS	Text	ROI Details
Investigative Techniques	C_INVESTIGATIVE_TECHNIQUES	Text	Investigative Techniques
ROI	C_ROI	File	ROI File Attachment
SA Signature	C_SA_SIGNATURE	Password	SA Signature

FECA Claims (T_FECA_CLAIMS)

FECA Claims

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Accommodated	C_ACCOMMODATED	Number	Accommodated
Age	C_AGE	Number	Age
Claimant #	C_CLAIMANT_	Text	Claimant #
COMP	C_COMP	Number	Comp
COMP Total	C_COMP_TOTAL	Currency	Comp Total
Current Address	C_CURRENT_ADDRESS	Text	Line 1 of claimant's current address - may be different from the address on file.
Date of Last	C_DATE_OF_LAST_VISIT	Date	Date on which

FECA Claims

Element Name	Column Name	Data Type	Description
Visit			claimant was last seen / interviewed.
District	C_DISTRICT	Number	District
DOB	C_DOB	Date	Claimant's date of birth.
DOS End	C_DOS_END	Date	Ending date of service.
DOS Start	C_DOS_START	Date	Starting date of service.
First Name	C_FIRST_NAME	Text	First name of claimant
Gender	C_GENDER	Number	Gender
Injury	C_INJURY	Text	Injury
Last Name	C_LAST_NAME	Text	Last name of claimant
MED	C_MED	Number	MED
MED Total	C_MED_TOTAL	Currency	Med Total
Middle Name	C_MIDDLE_NAME	Text	Middle name of claimant
Other Identifier	C_OTHER_IDENTIFIER	Text	Any identifying number or code that pertains to the claimant other than SSN or VIDA number.
POS Location	C_POS_LOCATION	Number	Post of Service Location
POS Region	C_POS_REGION	Number	Region
Pre-existing Condition	C_PREEXISTING_CONDITION	Text	Pre-existing Condition
SSN	C_SSN	Number	SSN
Status	C_STATUS	Text	Status of claimant as of last visit.
Survivor Benefit	C_SURVIVOR_BENEFIT	Number	Survivor Benefit
Time in Service	C_TIME_IN_SERVICE	Text	Time in Service

Evidence (T_EVIDENCE)

Evidence

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Comments	C_COMMENTS	Text	Comments
Disposition Date	C_DISPOSITION_DATE	Date	Date on which the evidence disposition occurred (e.g. returned or destroyed).
Document	C_DOCUMENT	File	Document
Document Date	C_DOCUMENT_DATE	Date	Document Date
Document Type	C_DOCUMENT_TYPE	Number	Document Type
Evidence Disposition	C_EVIDENCE_DISPOSITION	Number	Document / Evidence Disposition - returned, destroyed, etc.
Log Number	C_LOG_NUMBER	Text	Evidence log number for cross-reference.
Title	C_TITLE	Text	Title / name of document or other piece of evidence.

Activity Log (T_ACTIVITY_LOG)

Activity Log

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking

Activity Log

Element Name	Column Name	Data Type	Description
			object ID.
Activity	C_ACTIVITY	Text	Activity
Activity Date	C_ACTIVITY_DATE	Date	Activity Date
Activity Location	C_ACTIVITY_LOCATION	Text	Activity Location
Activity Type	C_ACTIVITY_TYPE	Number	Activity Type
Anticipated Completion Date	C_ANTICIPATED_COMPLETION_DATE	Date	Date that the activity is expected to be completed.
Completed	C_COMPLETED	Number	Completed

Admin Events (T_ADMIN_EVENTS)

Admin Events

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Admin Event	C_ADMIN_EVENT	Number	Admin Event
Comments	C_COMMENTS	Text	Comments
Event Date	C_EVENT_DATE	Date	Date

Case Disposition (T_CASE_DISPOSITION)

Case Disposition

Element Name	Column Name	Data Type	Description

Case Disposition

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Action Required	C_ACTION_REQUIRED	Yes/No	Action Required
Case Open Date	C_CASE_OPEN_DATE	Date	Case Open Date
CIRF Number	C_CIRF_NUMBER	Text	CIRF Number
Comments	C_COMMENTS	Text	Comments
Coordination	C_COORDINATION	Number	Indicates whether the investigation is a joint coordination w/ any other agency or department.
Date Closed	C_DATE_CLOSED	Date	Date Closed
Date Referred to Peace Corps	C_DATE_REFERRED_TO_PEACE_CORPS	Date	Date Referred to Peace Corps
Draft Report Date	C_DRAFT_REPORT_DATE	Date	Draft Report Date
Final Report Date	C_FINAL_REPORT_DATE	Date	Final Report Date
FOIA	C_FOIA	Number	FOIA
Investigation Number	C_INVESTIGATION_NUMBER	Text	Investigation number that was generated upon case

Case Disposition

Element Name	Column Name	Data Type	Description
			creation.
Investigation Status	C_INVESTIGATION_STATUS	Number	Investigation Status
Joint Investigation Agencies	C_JOINT_INVESTIGATION_AGENCIES	Text	Joint Investigation Agencies
Refer to USDOJ	C_REFER_TO_USDOJ	Number	Refer to USDOJ
SARC	C_SARC	Number	SARC

Subpoena (T_SUBPOENA)

Subpoena

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Inquiry (T_INQUIRY.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Comments	C_COMMENTS	Long Text	Comments
Date Due	C_DATE_DUE	Date	Date Due
Date Served	C_DATE_SERVED	Date	Date Served
Extension Granted To	C_EXTENSION_GRANTED_TO	Date	Extension Granted To
Issued To	C_ISSUED_TO	Text	Issued To
Received Date	C_RECEIVED_DATE	Date	Received Date
Subpoena #	C_SUBPOENA_	Text	Subpoena Number

Victim Address (T_VICTIM_ADDRESS)

Victim Address

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Victim (T_VICTIM.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Address Line 1	C_ADDRESS_LINE_1	Text	Address Line 1
Address Line 2	C_ADDRESS_LINE_2	Text	Address Line 2
Address Type	C_ADDRESS_TYPE	Number	Address Type
City	C_CITY	Text	City
Location	C_LOCATION	Number	Location
Region	C_REGION	Number	Region
State	C_STATE	Number	State
Zip Code	C_ZIP_CODE	Text	Zip Code

Subject Address (T_SUBJECT_ADDRESS)

Subject Address

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Subject (T_SUBJECT.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Address Line 1	C_ADDRESS_LINE_1	Text	Address Line 1
Address Line 2	C_ADDRESS_LINE_2	Text	Address Line 2
Address Type	C_ADDRESS_TYPE	Number	Address Type

Subject Address

Element Name	Column Name	Data Type	Description
City	C_CITY	Text	City
Location	C_LOCATION	Number	Location
Region	C_REGION	Number	Region
State	C_STATE	Number	State
Zip Code	C_ZIP_CODE	Text	Zip Code

Subject Disposition (T_SUBJECT_DISPOSITION)

Subject Disposition

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Subject (T_SUBJECT.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Cost Avoidance	C_COST_AVOIDANCE	Currency	Cost Avoidance
Date of Disposition	C_DATE_OF_DISPOSITION	Date	Date of Disposition
Date of Sentence	C_DATE_OF_SENTENCE	Date	Date of Sentence
Disposition	C_DISPOSITION	Number	Subject's final outcome with regard to the investigation.
Fine	C_FINE	Currency	Fine
IG Findings	C_IG_FINDINGS	Long Text	IG Findings
Recovery	C_RECOVERY	Currency	Recovery
Restitution	C_RESTITUTION	Currency	Restitution
Savings	C_SAVINGS	Currency	Savings
Sentence	C_SENTENCE	Text	Sentence
Venue	C_VENUE	Text	Venue

Contact Address (T_CONTACT_ADDRESS)

Contact Address

Element Name	Column Name	Data Type	Description
ID	ID	Numeric	Internal tracking identifier
ID_PARENT	ID_PARENT	Numeric	Foreign key reference to the Contacts (T_CONTACTS.ID)
ID_BASE	ID_BASE	Numeric	Foreign key reference to the base tracking object ID.
Address Line 1	C_ADDRESS_LINE_1	Text	Address Line 1
Address Line 2	C_ADDRESS_LINE_2	Text	Address Line 2
Address Type	C_ADDRESS_TYPE	Number	Address Type
City	C_CITY	Text	City
Location	C_LOCATION	Number	Location
Region	C_REGION	Number	Region
State	C_STATE	Number	State
Zip Code	C_ZIP_CODE	Text	Zip Code

APPENDIX MPE-B
PEACE CORPS OIG TRACKING SYSTEM TAB ACCESS PRIVILEGES BY ROLE

OIG TRACKING SYSTEM TAB ACCESS PRIVILEGES BY ROLE

The following grid is MPE's understanding of the user roles that should be available to the Peace Corps OIG tracking system and each role's associated tab access.

	IG System Roles				
Tab Name	Inspector General (Moderate Risk)	Admin (Highest Risk)	Agent (High Risk)	AIGI (High Risk)	PI Entry (Moderate Risk)
*Inquiry	Read only	Full access	Create and Read only	Full access	Full access
Victim	Read only	Full access	Full access	Read only	Full access
Victim Address	Read only	Full access	Full access	Read only	Full access
Subject	Read only	Full access	Full access	Read only	Full access
Subject Address	Read only	Full access	Full access	Read only	Full access
Subject Disposition	Read only	Full access	Full access	Read only	Full access
Activity Log	Read only	Full access	Create and Read only	Read only	**No Access**
Admin Events	Read only	Full access	Create and Read only	Read only	**No Access**
Case Disposition	Read only	Full access	Full access	Read only	**No Access**
Contacts	Read only	Full access	Full access	Read only	Full access
Contacts Address	Read only	Full access	Full access	Read only	Full access
Subpoena	Read only	Full access	Create and Read only	Read only	**No Access**
Investigative Plan	Read only	Full access	Full access	Full access	**No Access**
MOA / MOI	Read only	Full access	Full access	Full access	**No Access**
ROI	Read only	Full access	Full access	Full access	**No Access**
FECA Claims	Read only	Full access	Full access	Read only	**No Access**

Documents / Evidence	Read only	Full access	Full access	Read only	**No Access**
Assignments	Read only	Full access	Full access	Read only	Full access
Administrative Functions: Manage User Accounts, Manage User Groups, Manage User Roles, Manage System Reference Data	**No Access**	Full access	**No Access**	**No Access**	**No Access**
Audit Log, Event Log, and User Log reporting	Read only (reports are non-editable by default)	**No Access**	**No Access**	**No Access**	**No Access**