MS 899 Breach Notification Response Plan

Effective Date: October 8, 2024
Responsible Office: Office of Management/The Freedom of Information Act (FOIA); Privacy Act Office; Office of the Chief Information Officer (OCIO)
Supersedes: 08/01/16; 01/28/13; 01/7/13; 07/23/08

Issuance Memo (07/23/2008)
Issuance Memo (01/07/2013)
Issuance Memo (01/28/2013)
Issuance Memo (08/01/2016)
Issuance Memo (10/08/2024)

Table of Contents

1.0 Purpose

The purpose of this Manual Section is to set out Peace Corps policy regarding actions that must be taken when a "Breach" has occurred and "Personally Identifiable Information (PII)" in the possession or control of the Peace Corps has been or may have been compromised. (*See* definitions below.) This Manual Section constitutes the Peace Corps' Breach Notification Response Plan (Breach Plan).

2.0 Authorities

U.S. Department of Health and Human Services (HHS), Administrative Data Standards and Related Requirements, 45 Code of Federal Regulations (C.F.R.) § 160 and § 164 (August 31, 1981) (as amended July 8, 2024);
HHS, Health Information Technology for Economic and Clinical Health (HITECH) Act, 45 C.F.R § 170 (January 13, 2010);
Executive Order (E.O.) 13402, *Strengthening Federal Efforts to Protect Against Identity Theft*, 71

C.F.R. 27945 (May 10, 2006) (as amended November 3, 2006);
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 (December 17, 2022) (as amended December 18, 2014);
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 23, 2020);
NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (August 6, 2012) (as amended Revision 3, April 3, 2024 (draft));
Office of Management and Budget (OMB) Bulletin M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (September 2, 2016);
OMB Bulletin M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (June 15, 2017);
OMB Bulletin M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017);
OMB Circular A-130 Revision 4, *Managing Information as a Strategic Resource* (July 28, 2016);
OMB Bulletin M-24-04, *Fiscal Year Guidance on Information Security and Privacy Management Requirements* (December 4, 2023).

3.0 Definitions

For purposes of this Manual Section:

(a) ***Breach*** means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII, in any medium or form, including paper, oral, and electronic, or (2) an authorized user accesses or potentially accesses PII, in any medium or form, including paper, oral, and electronic, for an other than authorized purpose.

In the context of "Medically Confidential Information," as defined below, a Breach is the acquisition, access, use, or disclosure of an individual's Medically Confidential Information in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) that poses a significant risk of financial, reputational, or other harm to the individual.

(b) ***Personally Identifiable Information (PII)*** is paper, electronic, or oral information that can be used to distinguish or trace an individual's identity to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or an employee or contractor. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual.

(c) ***Sensitive Personally Identifiable Information (SPII)*** is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII requires stricter handling guidelines

because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements such as date of birth, Social Security numbers (SSNs), driver's license, state identification number, biometric records, financial or passport information, and criminal history. PII which is linked or linkable to a specific individual in combination with other data elements, such as address, telephone number, citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, or that poses a risk of identity theft are also SPII.

(d) ***Medically Confidential Information or Protected Health Information (PHI)***means oral or written information relating to the past, present, or future health, condition, care or treatment of a Peace Corps applicant, Trainee, Volunteer, or Peace Corps staff created or received by the Office of Health Services, a Peace Corps Medical Officer (PCMO), other Peace Corps health care provider, or any other Peace Corps staff authorized as having a need to know. It also includes information relating to the past, present, or future payment for such care.

(e) ***Incident*** means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(f) ***Major Incident*** is either:

(1) Any Incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. If the privacy Incident is validated as a Major Incident that involves PII, the Senior Agency Official for Privacy (SAOP), or their designee, must notify appropriate congressional committees no later than seven days after the date on which Peace Corps reasonably concluded that a major privacy Incident occurred. Agencies shall determine the level of impact of the Incident by using the existing Incident management process established by NIST, or

(2) A Breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

(g) ***Response Team*** means one or more of the following supervisory groups (collectively the "Response Teams") that may be involved in responding to Breaches of PII.

(1) A ***Core Response Team*** is formed when a Breach of PII involves a limited number of individuals and a limited amount of information. The Core Response Team shall, at a minimum, include the:

(i) SAOP, who is the Associate Director for the Office of Management,

(ii) Chief Information Officer;

(iii) General Counsel,

(iv) Associate Director for the Office of Safety and Security (OSS),

(v) Manager of the program or office experiencing the Breach, and

(vi) Privacy Act Officer (PAO).

(2) A ***Full Response Team.*** This Response Team is used when there is a major Breach involving a large amount of, or significant types of, PII. It includes the:

(i) SAOP,

(ii) Chief Information Officer and the CISO as required,

(iii) General Counsel,

(iv) Associate Director for the Office of Safety and Security,

(v) Manager of the program or office experiencing the Breach,

(vi) PAO,

(vii) Director of the Office of Communications,

(viii) Chief Human Capital Officer,

(ix) Director of Congressional Relations,

(x) Associate Director of Office of Global Operations,

(xi) Chief Compliance and Risk Officer,

(xii) Chief Financial Officer, and

(xiii) In Breaches involving Medically Confidential Information, the Associate Director of the Office of Health Services.

4.0 Policies

(a) All staff, including employees and contractors, and Volunteers/Trainees (V/Ts) shall immediately report any suspected or known Breach of PII, SPII, and/or Medically Confidential Information and follow the rules set out in this Manual Section.

(b) Staff and V/Ts shall relay the following basic information: date of the Incident, location of the Incident, what information was or may have been breached, nature of the Breach, and the suspected number of impacted individuals, if known.

(c) The Breach Plan policies are supplemented by the requirements for reporting and handling Breaches of electronic records and assets under the Cyber Incident Response Plan as set forth in MS 550 *Cybersecurity Incident Response Program*.

(d) Breach Plan requirements and responsibilities shall, as appropriate, be included in Peace Corps contracts and agreements to ensure that experts, personal services contractors (PSCs), and other contractors who use, access, or handle PII are similarly informed and held accountable.

5.0 Roles and Responsibilities

5.1 Director of the Peace Corps

The Director of the Peace Corps shall have the final decision-making authority with regard to notifying, offering guidance, and providing services to individuals affected by a Breach. The Director may designate senior leadership to make these final decisions. Any decision to delay notification to individuals affected by a Breach shall be made by the Director.

5.2 Response Teams

(a) In order to ensure an adequate response to a Breach, the Peace Corps has identified certain individuals who will be part of the Response Teams that address a Breach. The responsibilities of the Response Teams are to determine how to respond to a Breach. The nature and potential impact of the Breach determines whether the Core Response Team or the Full Response Team should be involved.

(b) The Response Team's mission is to provide planning, guidance, analysis, and a recommended course of action in response to a Breach. In the event of a Breach, the Response Team will be convened promptly to conduct a risk analysis to determine whether the Breach poses risks related to identity theft or other harms and will implement a timely, risk-based, tailored response to each Breach.

(c) The Response Team will coordinate with other Peace Corps offices, as appropriate, to ensure that timely, risk-based, tailored responses to data Breaches are developed and implemented. Responding to a particular Breach will likely require assistance from the managers and staff of the office or program that experienced the Breach. The Response Team will coordinate actions with the CISO's Security Incident Response Team (SIRT) when there has been a Breach of PII contained in electronic records or assets. (*See* MS 550 for additional information on the SIRT.)

(d) The Response Team will work closely with other federal agencies' offices and teams, as appropriate.

(e) If there has been a Breach of PII of a staff member or V/T, which was provided to the Peace Corps and then transmitted to another federal agency, the Response Team will monitor the remedial action taken by such agency and, as appropriate, the notifications made by the agency to affected parties.

5.3 Senior Agency Official for Privacy (SAOP)

SAOP is responsible for the following:

(a) Offering guidance to the Director and/or senior leadership during the Breach.

(b) Serving as the Chair of the Response Team, presiding over meetings and initiating responses to Incidents as appropriate.

(c) Oversight of all phases of the Peace Corps planning, preparation, investigation, and response to Breaches involving PII and SPII.

(d) Where there is a Breach, with the assistance of OSS, ensuring that necessary steps are taken to contain and control the Breach and prevent further unauthorized access to or use of PII. Such steps may include changing locks; deactivating facility access cards; enhancing physical security measures; alerting the Federal Protective Service; and/or developing or implementing special instructions, reminders, or training.

(e) Determining whether the Response Team should review the reported Incident to determine any other appropriate Peace Corps response.

(f) Deciding when potentially affected individuals should be notified.

5.4 Privacy Act Officer (PAO)

The PAO, or their designee, will provide subject matter expertise and operational support in analyzing and responding to a suspected or actual Breach. This includes, but is not limited to, scheduling meetings of the Response Teams, facilitating and recording their meetings, and providing meeting summaries. The PAO may also meet with affected program offices to determine the level of PII exposed by the Breach and report the findings to the SAOP and Response Team.

5.5 Office of Safety and Security

OSS is responsible for the restriction of physical access to Peace Corps space through the revocation of facility access cards and/or keys as appropriate. OSS is also responsible for the operation of the Insider Threat Program. *See* MS 404 *Insider Threat Program*.

5.6 Office of the Chief Information Officer (OCIO)

OCIO will take all necessary steps to contain, control, and mitigate the risks from a Breach involving information contained in IT systems and prevent further unauthorized access to or use of individual information, including as appropriate: (1) monitoring, freezing, or closing affected Peace Corps accounts; (2) modifying computer access codes; and (3) taking other necessary and appropriate action.

5.7 Chief Information Security Officer (CISO)

The CISO or their designee will function as the "Cybersecurity Incident Response Coordinator" and may delegate aspects of this function as necessary. (*See* MS 550.) After receiving an Incident Response Report, the CISO will complete the Report and forward it to the SAOP, PAO, and the Office of Inspector General. The CISO will also forward it to the U.S. Computer Emergency Readiness Team (U.S. CERT) for external reporting as soon as possible after the first notice of the suspected or confirmed Breach.

5.8 Office of the General Counsel

The Office of the General Counsel is responsible for providing all legal support and guidance with regard to any suspected or actual Breach.

5.9 Office of External Affairs

5.9.1 Director of the Office of Communications

In the case of a Breach, the Director of the Office of Communications, in coordination with the Response Team, and with approval from the Director's office, is responsible for directing all meetings and discussions with the news media and the public. This includes the issuance of press releases and related materials on the agency's website.

5.9.2 Office of Congressional Relations

The Office of Congressional Relations, in consultation with the Response Team, is responsible for coordinating all communications and meetings with members of Congress and their staff.

5.10 Office of Inspector General (OIG)

The role of the OIG is to provide oversight of the agency's Incident response, investigate Breaches as appropriate, and review relevant information to independently evaluate the Peace Corps response to a Breach. To report an Incident to the OIG, staff and V/Ts should call the OIG hotline numbers at 202-692- 2915 or 800-233-5874, via email at oig@peacecorpsoig.gov, or online at https://www.peacecorpsoig.gov/contact/hotline.

6.0 Response Actions

6.1 Initial Notification of Breach

(a) **Domestically**: Whenever there is a suspected or known Breach domestically, the staff member shall promptly notify the Peace Corps Service Desk by calling +1- 202-692-1000 and notifying their immediate supervisor.

(b) **Overseas**: Whenever there is a suspected or known Breach overseas, the staff member or V/T shall promptly notify the Post's IT Specialist. The Post's IT Specialist shall promptly notify the Service Desk by calling +1-202-692-1000 and their immediate supervisor.

6.2 Convening the Response Team

Within 24 hours of being notified of an Incident, involving or potentially involving PII, SPII, or Medically Confidential Information, the SAOP shall first determine whether the agency's response can be conducted at the staff level or whether the agency must convene a Response Team.

The Response Team shall evaluate the available information to help determine whether PII has been compromised or potentially compromised and how to respond. The Response Team should gather as much information as possible and update their records as facts and information become available or are revised.

As part of any initial evaluation, the following issues shall be investigated:

(a) The date of the Incident;

(b) The nature and means by which the Breach occurred, such as:

  (1) Whether the Breach is suspected or confirmed,

  (2) The circumstances surrounding the suspected or confirmed Breach, including the type of information that constitutes PII,

  (3) The purposes for which the PII is collected, maintained, and used,

  (4) The length of time the PII was exposed,

  (5) The format of the PII (structured or unstructured),

  (6) Whether there was unauthorized access to or use of information,

  (7) Whether there was a lost computer, storage device, or portable media,

  (8) Whether there was a system or network intrusion, and

  (9) Whether there was loss of control of paper documents containing sensitive information;

(c) Who reported or discovered the Incident;

(d) The number of individuals potentially affected;

(e) The accessibility of the information; and

(f) The strength and level of encryption of the security technologies that are protecting the data.

6.3 Assessing the Risk of Harm to Individuals Potentially Affected by a Breach to Determine Whether Notification is Required

The SAOP, in cooperation with the Response Team, shall conduct and document an assessment of the risk of harm to individuals potentially affected by a Breach. The SAOP shall consider the potential harms that may result from the loss or compromise of PII. This includes, but is not limited to, Breaches of confidentiality, blackmail, disclosure of private information, mental pain, emotional distress, financial harm, potential for secondary use, or unwarranted exposure leading to humiliation or loss of self-esteem.

6.3.1 Factors Involved in Risk Assessment

When assessing the risk of harm, the SAOP shall consider the following factors:

(a) The nature and sensitivity of PII, including:

(1) The sensitivity of each individual data element. Examples of data elements include, but are not limited to, SSNs, Volunteer IDs, passport numbers, driver's license numbers, bank account numbers, passwords, and biometric identifiers. In addition to evaluating the sensitivity of each data element individually, the SAOP shallevaluate the sensitivity of all the data elements together;

(2) The context of the PII. This includes the purpose for which the PII was collected, maintained, and used;

(3) The extent to which the PII constitutes information that an individual would generally keep private. Examples of private information include, but are not limited to, derogatory personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, immigration status, and passwords;

(4) Whether the potentially affected individuals are from a particularly vulnerable population. Examples include, but are not limited to, children, V/Ts, host families, confidential informants, witnesses, and victims of certain crimes that may occur in a host country where V/Ts are serving;

(5) The permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Special consideration is warranted when a Breach involves biometric information. When considering the nature and sensitivity of biometric information, an agency shall factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated; and

(6) The likelihood that the PII was accessed or misused.

(b) The likelihood the information is accessible and usable, including:

(1) Security safeguards, such as encryption methods;

(2) Format and media;

(3) Duration of exposure; and

(4) Evidence of misuse. Such evidence may determine with a high degree of certainty that PII has been or is being misused. Furthermore, evidence may determine with reasonable certainty that the PII was not misused.

(c) The type of Breach, including the:

(1) Whether the Breach was intentional, unintentional, or whether the intent is unknown; and

(2) Who received the compromised PII. This knowledge may assist the SAOP in assessing the likely risk of harm to individuals. Inadvertent disclosures to known individuals either internal to Peace Corps or external to Peace Corps may result in a minimal risk of harm to the compromised individuals. However, if analysis reveals that the PII is under the control of a group or individual who is either untrustworthy or known to exploit compromised information, the risk of harm to the compromised individual is considerably higher.

6.4 Determining Whether Notification is Required for Medically Confidential Information

For Medically Confidential Information, an individual shall be notified where disclosures not authorized under HIPAA regulations pose a significant risk of financial, reputational or other harm to the individual.

6.5 Determining if Breach Causes Identity Theft Risks

To determine if a Breach causes identity theft risks, the Response Team shall evaluate certain factors including:

(a) The type of information that was compromised;

(b) How well the information was protected from unauthorized access;

(c) The means by which the loss occurred, including whether the Incident might be the result of criminal activity or is likely the result of criminal activity;

(d) The ability of the Peace Corps to mitigate the identity theft; and

(e) Evidence that the compromised information is being used to commit identity theft.

6.6 Other Potential Harms

Even if there is no risk of identity theft, the Response Team shall consider a wide range of potential harms and determine whether external notification of a Breach is necessary. The Peace Corps is legally required to protect against any anticipated threats or hazards to the security or integrity of records, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Additionally, the Response Team may consider a number of possible harms associated with the loss or compromise of information. For example, such harms may include the effect of a Breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, and the potential for secondary uses of the information which could result in fear or uncertainty.

Notification of a Breach involving Medically Confidential Information is required where there is a significant risk of financial, reputational or other harm to the individual.

6.7 Impact Levels

The Response Team shall review and assess the level of impact already assigned to the information using the impact levels defined by NIST. The three impact levels below describe the potential impact on an organization or individual if a Breach of security occurs.

(a) **Low** means the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

(b) **Moderate** means the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

(c) **High** means the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

6.8 Mitigation of the Risk of Harm to Individuals Potentially Affected by a Breach

Once the SAOP assesses the risk of harm to individuals potentially affected by a Breach, the SAOP, in coordination with the Response Team when applicable, shall consider how best to mitigate the identified risks.

The SAOP shall determine and document the actions that the agency will take to mitigate the risk of harm. These actions can include:

(a) Countermeasures (e.g., requiring all users to automatically change their passwords should they be compromised during a Breach),

(b) Providing guidance (e.g., how individual can request a free credit report), and/or

(c) Providing services (e.g., providing identity monitoring and credit monitoring through an approved agency contract).

6.9 Notification

The Full Response Team will determine the notification necessary for any Major Incident. The Core Response Team will make a recommendation to the PAO, or their designee, regarding other Breaches, and the PAO will then make a recommendation to the SAOP.

When considering whether notification of a Breach is necessary, the Response Team will determine the scope of the Breach, to include the types of information exposed, the number of people impacted, and whether the information could potentially be used for identity theft or other similar harms. The Response Team will also assess the likely risk of harm caused by the Breach and will assess the level of risk and consider a wide range of harms that include harm to reputation and potential risk of harassment, especially when health or financial records are involved.

6.9.1 Delaying Notification of Affected Individuals

Under circumstances where there is little or no risk of harm and where notification could increase such a risk, the prudent course of action may be to delay or forgo notification while appropriate safeguards are put in place.

6.9.2 When Notification is Appropriate

If the Response Team determines that notification of the Breach is appropriate, it shall consider the following factors:

(a) The timing of the notification. A notification will be issued without unreasonable delay following the discovery of a Breach. However, any delay should not exacerbate risk or harm to any affected individuals. Notifications in the context of Medically Confidential Information must be made within 60 days of discovery of the Breach;

(b) The source of the notification. Notification to individuals should generally be issued by the Director or a senior-level individual designated by the Director in writing; and

(c) The contents of the notification shall include the following:

(1) A brief description of what happened, including the date(s) of the Breach and of its discovery;

(2) To the extent possible, a description of the types of personal information that were involved in the data security Breach (e.g., full name, SSN, date of birth, home address, account number, disability code, etc.);

(3) A statement whether the information was encrypted or protected by other means, when it is determined by the Freedom of Information Act (FOIA) and Privacy Act Office

(Privacy Act Office) or the IT Security staff, that such information would be beneficial and would not compromise the security of the system;

(4) Steps individuals should take to protect themselves from potential harm, if any;

(5) Any agency action to investigate the Breach, mitigate losses, and to protect against any further Breaches; and

(6) How affected individuals should contact the agency for more information, including a toll-free telephone number, email address, and postal address.

6.9.3 Timeframe for Communication to Impacted Individuals.

Unless directed to delay, initial notification to impacted individuals shall be completed within ninety (90) calendar days of the date upon which the Incident was reported. In the event the communication could not occur within this timeframe, the PAO, or their designee, will notify the SAOP explaining why communication could not take place within this timeframe and will submit a revised timeframe and plan explaining when communication will occur.

6.9.4 Translation of Notification into Other Languages or Formats

Effective privacy Incident handling necessitates that individuals affected by the privacy Incident understand the importance of the notification. Therefore, if the record shows that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). If the agency has knowledge that the affected individuals are not English speaking, or require translation services, the individual should also be provided translation services in the appropriate languages to the extent feasible. Special consideration should be given to provide notification to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a telecommunications device for the deaf (TDD) or posting a large type notice on the Peace Corps' website.

6.9.5 Establishing a Call Center

For an Incident that affects a large number of individuals, or as otherwise appropriate, the agency may establish a toll-free call center staffed by trained personnel to handle inquiries from the affected individuals.

6.9.6 Notification to Third Parties

Notification to individuals and to third parties, including the timing, order, and content of such notice, shall be carefully coordinated so that ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Notice to the media and the public, financial institutions, and appropriate members of Congress may be considered depending upon the nature of the Breach.

6.9.6.1 Notifications to Financial Institutions

In the case of a Breach that involves government-authorized credit cards, the Peace Corps must notify the issuing bank promptly, and the Response Team shall coordinate with the Office of the Chief Financial Officer regarding such notification and suspension of the account. If the Breach involves individuals' bank account numbers that are used in employment or V/T-related transactions, the Peace Corps will notify the bank or other entity that handles that particular transaction for the agency. If the Breach involves PSCs or vendors operating in host countries, the SAOP, or their designee, will coordinate notification with the Department of State.

6.10 Closure

Once mitigation for the Incident is completed, the PAO, or their designee, shall update the report and recommend Incident closure. This recommendation is subject to review by the SAOP. However, the ultimate decision to close the Incident rests with the SAOP. Until this determination is reached, and the SAOP notifies the PAO, or their designee, that the Incident is closed, the Incident will remain open for review or further Incident handling.

6.11 Documentation of Breach Notification Response

The Response Team, in coordination with the Agency Records Officer, OGC, and any other appropriate officials and staff, shall ensure that appropriate and adequate records are maintained to document the Response Team's response to all Breaches reported under this plan. Such records shall be destroyed only in accordance with the General Records Schedule.

6.12 Lessons Learned

The PAO, or their designee, will conduct a "lessons learned" exercise, when appropriate, which underscores the importance of maintaining the Incident record through each activity and can enable the Peace Corps to implement specific, preventative actions to protect and safeguard PII.

This exercise should review the Incident to determine whether its root cause can be identified. By identifying the root cause, the Peace Corps can identify potential ways to enhance or strengthen staff and V/T awareness through training or awareness campaigns, as well as potential changes to policies or procedures to assist Peace Corps staff and V/Ts in safeguarding PII.

7.0 Tracking and Documenting the Response to a Breach

The SAOP, or their designee, shall develop and maintain a formal process to track and document each Incident, including Breaches, reported within the Peace Corps. The Privacy Act Office must track and monitor the following:

(a) The total number of Breaches reported over a given period of time;

(b) The status for each reported Breach, including whether the response to a Breach is ongoing or has concluded;

(c) The number of individuals potentially affected by each reported Breach;

(d) The types of information potentially compromised by each reported Breach;

(e) Whether the Peace Corps, after assessing the risk of harm, provided notification to the individuals potentially affected by a Breach;

(f) Whether the Peace Corps, after considering how to mitigate the identified risks, provided services to the individuals potentially affected by a Breach; and

(g) Whether a Breach was reported to the U.S. CERT and/or Congress.

8.0 Evaluation of Breach Response

The development and implementation of this Breach Plan is an ongoing process. Accordingly, following the handling and disposition of all suspected or actual Breaches reported under this plan, the Response Team will assess its response, identify tasks that could have been conducted more effectively and efficiently, and make improvements or modifications to the Breach Plan as appropriate.

The Response Team will meet at least once per year, and more regularly when a Breach occurs, to discuss employee training and the status of Breaches at the Peace Corps.

9.0 Annual Report

The SAOP completes the annual report for the agency, as required under FISMA.

10.0 Annual Breach Response Plan Reviews

At the end of each fiscal year, the SAOP shall review reports detailing the status of each Breach reported during the fiscal year and consider whether it is necessary to take action, including, but not limited to:

(a) Updating the Breach notification response plan;

(b) Developing and/or implementing new, or revising existing, policies to protect the agency's PII holdings;

(c) Reinforcing or improving training and awareness;

(d) Modifying information sharing arrangements; and/or

(e) Developing or revising documentation or privacy policies.

11.0 Training

The PAO will provide training regarding responsibilities for safeguarding PII. Such training must be completed prior to obtaining access to information and annually to ensure individuals are up-to-date on the proper handling of PII. Failure to complete required training may result in denial of access to information.

12.0 Disciplinary Action

(a) Any Peace Corps employee who has been trained and does not meet their responsibilities to safeguard PII may be subject to appropriate disciplinary action that may include reprimand, suspension, removal, or other actions in accordance with applicable laws and Peace Corps policy.

The following may lead to disciplinary action:

(1) Failure to implement and maintain security controls for PII, for which an employee is responsible, regardless of whether the employee causes the loss of control or unauthorized disclosure of PII;

(2) Exceeding authorized access to, or disclosure to unauthorized persons of, PII;

(3) Failure to report any known or suspected loss of control or unauthorized disclosure of PII; and

(4) for managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

Any temporary employee or expert consultant who has been trained and does not meet his or her responsibilities to safeguard PII may be subject to termination of their appointment.

(b) Any contractor who has been trained and does not meet their responsibilities to safeguard PII may be subject to action consistent with the terms of the relevant contract.

13.0 Effective Date

The effective date of this Manual Section is the date of issuance.