MS 899 BREACH NOTIFICATION RESPONSE PLAN

Date: July 23, 2008
Responsible Office: M/FOIA & Privacy Office
New Manual Section

Issuance Memo

TABLE OF CONTENTS

1.0 Authorities
2.0 Purpose
3.0 Definitions
4.0 Policies
5.0 Breach Notification Response Team
5.1 Response Team Membership
5.2 Responsibilities of Core Team Members
6.0 Procedures
6.1 Initial Notification of Breach
6.2 Cyber Incident Response Report
6.3 Roles and Functions
6.4 Convening the Response Team
6.5 Intentional or Unintentional Loss of Control or Disclosure
6.6 Determining Whether Notification is Required
6.7 Determining if Breach Causes Identity Theft Risks
6.8 Other Potential Harms
6.9 Impact Levels
6.10 Ability of the Agency to Mitigate the Risk of Harm
6.11 Notification
6.11.1 Delaying Notification of Individuals
6.11.2 When Notification is Appropriate
6.11.3 Notification to Third Parties
6.11.4 Documentation of Breach Notification Response
6.12 Evaluation of Breach Response
7.0 Training
8.0 Disciplinary Action
9.0 Effective Date

1.0 AUTHORITIES

Executive Order 13402, May 2006; Office of Management and Budget (OMB) Memorandum, May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

2.0 PURPOSE

The purpose of this manual section is to set out the policies and procedures of the Agency's Breach Notification Response Plan (Breach Plan). The Breach Plan addresses incident reporting, incident response, the Breach Notification Response Team; external notification of breaches, training requirements, and consequences of breaches by staff.

3.0 DEFINITIONS

3.1 ***Personally Identifiable Information*** is information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security Number, or biometric records, alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

3.2 ***Covered Information*** means Personally Identifiable Information that poses a risk of identity theft. Covered Information includes, at a minimum, the following information, whether on paper, in electronic form, or oral communication:

(a) An individual's Social Security Number alone or

(b) An individual's name, address, or phone number in combination with one or more of the following: date of birth, Social Security Number, driver's license number, other state identification number or foreign country equivalent, passport number, or financial account number or credit or debit card number.

3.3 ***Breach and/or Incident*** means loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to Personally Identifiable Information or Covered Information, whether physical or electronic.

4.0 POLICIES

4.1 It is Peace Corps' policy that all Agency officials, employees, contractors, and Volunteers shall immediately report any suspected or known breach of Personally Identifiable Information and/or Covered Information (paper and/or electronic) to their managers and follow the procedures set out in this manual section.

4.2 The Breach Notification Response Plan policies and procedures supplement current requirements for reporting and handling Peace Corps' Cyber Incident Response Plan.

4.3 Breach Plan requirements and responsibilities shall, as appropriate, be included in Peace Corps' contracts and agreements to ensure that experts, personal services contractors, and other contractors who use, access, or hold personally identifiable information are similarly informed and held accountable.

5.0 BREACH NOTIFICATION RESPONSE TEAM

To mitigate the risk of harm (including identity theft), should a data breach occur, a Breach Notification Response Team (Response Team) is established to respond to the loss of certain categories of Personally Identifiable Information and/or Covered Information. The Response Team includes a sub-unit is entitled

the "Cyber Incident Response Team" (Cyber Response Team). The Cyber Response Team is the first responder to a suspected or known breach and is generally made up of IT security specialists.

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.

The Response Team will be convened to evaluate any potential breach and to help guide the Peace Corps' response. The Response Team should include staff with expertise in information technology; legal authorities, including law enforcement; the Privacy Act; or other area of expertise necessary to respond to a data breach.

5.1 Response Team Membership

The Response Team should, at a minimum, include a core group that includes the Agency's Chief Information Officer, General Counsel, and the Chief Privacy Officer. (The Associate Director for Management shall have the title and responsibilities of the Chief Privacy Officer.)

A full Response Team shall consist of the following officials or their designees: the manager of the program or the office experiencing the breach, the Chief Information Officer (CIO), Chief Privacy Officer (CPO), the Director of the Office of Communications/Press Relations, the Director of the Office of Congressional Relations, the General Counsel (GC), the Director of the Office of Human Resource Management (HRM), the Chief Compliance Officer, the Associate Director of the Office of Safety and Security (SS), and the Chief Financial Officer (CFO).

5.2 Responsibilities of Core Team Members

5.2.1 The CPO is responsible for serving as the chair of the Response Team, presiding over meetings and initiating responses to incidents as appropriate (the CIO will serve as the co-chair of the Response Team). The CPO is also responsible for participating in all phases of the Agency's planning, preparation, investigation, and response to breaches involving Personally Identifiable Information and Covered Information.

5.2.2 The Privacy Office will provide subject matter expertise and operational support in analyzing and responding to a suspected or actual breach.

5.2.3 The OGC shall be responsible generally for providing legal support and guidance in responding to a suspected or actual breach.

5.3 The Response Team will coordinate with other Peace Corps offices, as appropriate, to ensure that appropriate 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.

5.4 The Response Team will work closely with other federal agencies, offices, and teams, as appropriate.

6.0 PROCEDURES

6.1 Initial Notification of Breach

When there is a suspected or known breach domestically, a domestic staff member or contractor shall promptly notify the Domestic Service Desk by calling 1-202-692-1000.

When there is a suspected or known breach overseas, a staff member, contractor, or Volunteer shall notify the post's IT specialist. The IT specialist shall promptly notify the Domestic Service Desk by calling 1-202-692-1000.

6.2 Cyber Incident Response Report

Upon notification of an incident, the Domestic Service Desk shall fill out the top portion of the Cyber Incident Response Report located on the Office of IT Security intranet webpage and assign the incident to the Office of IT Security queue.

After receiving the Cyber Incident Response Report, the CIO's Incident Response Coordinator will assemble a Cyber Incident Response Team (Cyber Response Team). The Incident Response Coordinator will choose team members as necessary based on the initial reports and requests of systems affected.

The Cyber Response Team will complete the Cyber Incident Response Report and forward it to the FOIA/Privacy Office, the Chief Privacy Officer, and the Inspector General. The Cyber Report shall also be forwarded to the U.S. Computer Emergency Readiness Team (U.S.-CERT) for external reporting within one hour of the first notice of the breach. The Associate Director for Management shall have the title and responsibilities of the Chief Privacy Officer.

The Inspector General must independently evaluate the Agency's breach notification response plan. When applicable, the Inspector General, in accordance with responsibilities set forth in the Inspector General Act, may decide to investigate a breach. To report an incident to the OIG, call the IG hotline numbers at 202-692-2911, 2915, or 800-233-5874.

6.3 Roles and Functions

Based on initial reports, the Chief Privacy Officer will determine whether the Response Team should review the reported incident to determine any other appropriate Agency response.

The Office of the Chief Information Officer will take all necessary steps to contain, control, and mitigate the risks from the breach 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. Without undue delay, the Chief Information Officer shall take steps consistent with current requirements under the Federal Information Security Management Act (FISMA).

The restriction of physical access to space through the revocation of facility access cards and/or keys will be controlled by the Office of Safety and Security.

When there is a breach, including paper records and physical security that may affect an individual's privacy, the Peace Corps' Chief Privacy Officer, with the assistance of the Office of Safety and Security, shall ensure that necessary steps are taken to contain and control the breach and prevent further unauthorized access to

or use of individual information. 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. The CIO, in consultation with OGC, will handle the response to a potential or actual compromise of nonpublic information that does not concern personal privacy. The response must be consistent with the requirements of FISMA and other legal authorities.

6.4 Convening the Response Team

Within 24 hours of being notified of an incident involving or potentially involving Covered Information or Personally Identifiable Information by the OIG, the Chief Privacy Officer will, as appropriate, convene a meeting of the Response Team.

The Response Team will evaluate the available information to help determine whether data have been compromised or potentially compromised and how to respond.

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

(a) Date of incident;

(b) Nature of incident and the means by which the breach occurred;

(c) Unauthorized access to information;

(d) Unauthorized use of information;

(e) Lost computer, storage device, or portable media;

(f) System or network intrusion;

(g) Loss of control of paper documents containing sensitive information;

(h) Person who reported incident;

(i) Person who discovered incident;

(j) Number of individuals potentially affected; and

(k) The accessibility of the information.

6.5 Intentional or Unintentional Loss of Control or Disclosure

If an incident appears to involve the unintentional loss of control or disclosure of Personally Identifiable Information or Covered Information, the OCIO shall have primary responsibility for conducting an inquiry into the circumstances surrounding the loss.

If an incident appears to involve the intentional disclosure of Personally Identifiable Information or Covered Information or possible criminal activity related to a breach, the OIG shall be notified.

6.6 Determining Whether Notification is Required

To determine whether notification of a breach is required, the Response Team will assess the likely risk of harm caused by the breach and the level of risk. To assess the likely risk of harm, the following factors should be considered:

(a) Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. The data elements should be considered in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals;

(b) Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) chosen for providing notification, but should not be the determining factor for whether an agency should provide notification;

(c) Likelihood the Information is Accessible and Usable. Upon learning of a breach, the Agency should assess the likelihood Personally Identifiable Information will be or has been used by unauthorized individuals. The Response Team should consider whether the information has been encrypted, for example; and

(d) Likelihood the Breach May Lead to Harm. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the types of data involved in the incident.

6.7 Determining if Breach Causes Identity Theft Risks

To determine if a breach causes identity theft risks, the Response Team should evaluate the factors identified in the 2006 OMB Memo**.** These factors include:

(a) The type of Covered Information that was compromised;

(b) How easy or difficult it would be for an unauthorized person to access the information given how it was protected;

(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 actually being used to commit identity theft.

6.8 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 Privacy Act requires the Agency 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.

6.9 Impact Levels

The Response Team shall also review and assess the level of impact already assigned to the information using the impact levels defined by the National Institute of Standards and Technology (NIST). The three impact levels (low, moderate, and high) describe the potential impact on an organization or individual if a breach of security occurs:

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

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

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

6.10 Ability of the Agency to Mitigate the Risk of Harm

Within an information system, the risk of harm will depend on how Peace Corps is able to mitigate further compromise of the information and/or system(s) affected by a breach. In addition, countermeasures to contain the breach or its impacts should be considered. This could include monitoring other appropriate systems for misuse.

6.11 Notification

6.11.1 Delaying Notification of Individuals

Notification where there is little to no risk of harm might create unnecessary concern and confusion. Under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

6.11.2 When Notification is Appropriate

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

(a) Timing of Notification. A notification will be issued without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement, including the OIG, national security, and any measures necessary for the Agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised. Decisions to delay notification will be made by the Director of the Peace Corps or his or her designee, in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s);

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

(c) Contents of the Notice. The contents of the notice given by the Peace Corps to individuals shall include the following:

(1) A brief description of what happened;

(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.) and a statement whether the information was encrypted or protected by other means, when it is determined by the FOIA/Privacy Office or the IT Security staff, that such information would be beneficial and would not compromise the security of the system;

(3) Options individuals can take to protect themselves from identity theft, e.g., contacting financial institutions; monitoring financial account activity; requesting a free credit report; placing an initial fraud alert on credit reports; for residents of states in which it is authorized under state law, considering placing a freeze on their credit file; reviewing resources at www.idtheft.gov.

(d) Means of Notification. The best means for notifying affected individuals or others will depend on the number of individuals affected and the available contact information. The means used should be commensurate with the number of people affected and the urgency with which they need to receive notice. Among possible means are:

(1) Telephone - if used, it should be in conjunction with first-class mail notification;

(2) First-Class Mail - to the last known mailing address in Agency records. This should be the primary means of notification;

(3) E-Mail - can be used in conjunction with other methods. If the only available contact information is an e-mail address, then use this;

(4) Existing government-wide services, such as www.USA.gov and 1-800-FedInfo;

(5) Newspapers or other public media outlets, including call centers;

(6) Substitute Notice - where individual contact information is unavailable, posting on websites and using print and broadcast media may be appropriate. This should include a toll-free number where individuals can find out whether their information is included in the breach; and

(7) Accommodations - Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given.

6.11.3 Notification to Third Parties

Notice 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 following third parties may be considered depending on the nature of the breach and the following:

(a) Media and the Public. 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.

(b) Financial Institutions. If the breach involves government-authorized credit cards, the Peace Corps must notify the issuing bank promptly as set forth in the 2007 OMB Memo. The Response Team shall coordinate with the OCFO regarding such notification and suspension of the account. If the breach involves individuals' bank account numbers that are used in employment or volunteer-related transactions, the Peace Corps will notify the bank or other entity that handles that particular transaction for the Agency.

(c) Appropriate Members of Congress. 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.

If communicating with third parties regarding a breach is necessary, the Peace Corps will consider the following:

(a) Careful Planning. The Peace Corps' decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public or undermine any OIG coordination with law enforcement or prosecutorial entities. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust;

(b) Web Posting. The CPO will generally post information about the breach and notification in a clearly identifiable location on the home page of its web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting may include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process. The information could, if appropriate, also appear on the www.USA.gov web site;

(c) Notification of other Public and Private Sector Agencies. Other public and private sector agencies may need to be notified on a need-to-know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harm stemming from the breach.

6.11.4 Documentation of Breach Notification Response

The Response Team, in coordination with the Records Management Office, 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 Evaluation of Breach Response

The development and implementation of this Breach Notification Response Plan is an ongoing process, not a one-time exercise. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this plan, the Response Team will evaluate its response, identify tasks that could have been

conducted more effectively and efficiently, and make improvements or modifications to the Breach Notification Response Plan as appropriate.

The Response Team will meet regularly when an incident takes place and meet once per year to discuss employee training and the status of data breaches at the Agency.

7.0 TRAINING

The Peace Corps will train managers, supervisors, employees, and contractors regarding their responsibilities for safeguarding Personally Identifiable Information. For example:

(a) Employees and contractors will be trained on how to respond to and report a potential or confirmed data breach;

(b) Formal incident response procedures shall be part of the Peace Corps' mandatory annual IT security awareness and privacy training;

(c) Supervisors will attend privacy awareness training sessions during the HRM sponsored supervisor training and overseas training programs held at headquarters; and

(d) Privacy awareness training will be included as part of new employee orientation.

8.0 DISCIPLINARY ACTION

Any Peace Corps employee who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to appropriate disciplinary action. Any contractor who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to action consistent with the terms of the relevant contract. Any temporary employee or expert consultant who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to termination of their appointment.

9.0 EFFECTIVE DATE

The effective date is the date of issuance.