USAID
FROM THE AMERICAN PEOPLE

USAID Privacy Program
Breach Notification Policy and Plan

A Mandatory Reference for ADS Chapter 508

New Edition Date: 03/07/2014
Responsible Office: M/CIO/IA
File Name: 508mai_030714

Management Bureau/Chief Information Officer/Information Assurance
(M/CIO/IA)

USAID PRIVACY PROGRAM
BREACH NOTIFICATION POLICY

Version 2F

November 19, 2013

DOCUMENT CHANGE HISTORY

The table below identifies all changes incorporated into this template. Baseline changes require review and approval. The version states the number with either D for draft or F for final.

Change #	Date	Version #	Description
1.	November 6, 2012	1F	Created document.
2.	September 20, 2013	1F	Document Verified for accuracy. No changes needed.
3.	November 19, 2013	2F	Document updated as mandatory reference for ADS 508.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

This document provides the Privacy Program Breach Notification Policy.

1.2 SCOPE

This Policy applies to all employees and all bureaus, offices, and missions of the United States Agency for International Development (USAID).

Although most incidents involve information technology, a privacy breach may also involve physical security considerations (such as with paper documents, removable media, mobile devices) that may cause the compromise of PII.

1.3 BACKGROUND

USAID must manage, in accordance with Federal laws and regulations, the information it collects, uses, maintains, and disseminates in support of its mission and business functions. Some information, such as PII, requires additional protection due to its sensitivity and the risks of misuse associated with a potential unauthorized disclosure.

USAID is responsible for safeguarding the PII in its possession and for preventing the breach of PII entrusted to the Agency. Any unauthorized use, disclosure, or loss of PII can result in the loss of the public's trust and confidence in the Agency's ability to properly protect such information. In addition to efforts to ensure proper PII safeguards, USAID must have an appropriate PII breach notification policy to mitigate any potential harm caused by any PII breaches.\

PII breaches may have far-reaching implications for the individuals whose PII is compromised, including identity theft which might result in financial loss and/or personal hardship to the individual. A PII breach may also require significant USAID staff, time, assets, and financial resources to mitigate, which may prevent the Agency from allocating those resources elsewhere. USAID is responsible for mitigating the risks associated with the inadvertent loss, or unapproved use or disclosure of PII. Protecting PII in the possession of USAID and preventing its breach are necessary to ensure that USAID retains the trust of the American public.

In compliance with the May 22, 2007, OMB Memorandum M-07-16, entitled *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* USAID has established this Privacy Program Breach Notification Policy. This Policy ensures that USAID responses to PII breaches are consistent, comprehensive, complete, and delivered in an effective and timely manner, in order to minimize risk to individuals and the Agency.

2. ROLES AND RESPONSIBILITIES

2.1 SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)

The Senior Agency Official for Privacy (SAOP) develops and ensures the implementation of the USAID Privacy Program Breach Notification Policy. The SAOP is the Chair of the Breach Response Team (BRT), and is responsible for notifying, as appropriate, the BRT, the Assistant Administrator for the Bureau for Management, and the Administrator of the occurrence of a breach. The SAOP coordinates privacy breach activities with the Inspector General, as appropriate; and serves as the contact point for the Office of Management and Budget and Congress on all matters pertaining to breach notification actions.

2.2 USAID BREACH RESPONSE TEAM (BRT)

The USAID Breach Response Team (BRT) is comprised of senior officials or their delegates, including the SAOP as Chair, Chief Privacy Officer (CPO), Chief Information Officer (CIO), CISO, Inspector General, General Counsel, Assistant Administrator for the Bureau of Legislative and Public Affairs, Chief Financial Officer, Senior Procurement Executive and Director of the Office of Acquisition and Assistance, and the Program Manager for the program that is experiencing the breach.

The BRT is responsible for ensuring that appropriate privacy breach notifications are made to the affected individuals as quickly as feasible. The BRT coordinates breach notification issues across USAID at the senior official level. The BRT will implement privacy breach notification activities to ensure that such activities are commensurate with the impact to the individual and comply with applicable federal legal authorities.

2.3 CHIEF PRIVACY OFFICER (CPO)

The Chief Privacy Officer (CPO) is responsible for implementing the USAID Privacy Program Breach Notification Policy by developing the privacy program procedures on privacy breach assessment, response, and notifications. The CPO will ensure that privacy breaches are identified, tracked, and responded to in an effective, consistent, and timely manner.

The CPO provides the operational support for the BRT, submits recommendations to the BRT on Agency responses to specific breaches, and prepares critical review and analysis of breach activities. The CPO coordinates breach notification issues across USAID at the operational level. The CPO also coordinates with USAID ISSOs, USAID CSIRT, and provides guidance to USAID personnel in evaluating and reporting suspected or confirmed incidents involving PII.

2.4 PRIVACY OFFICE

The Privacy Office is comprised of Privacy Analysts who engage in privacy incident risk analysis, under the supervision of the CPO. The Privacy Analyst assigned to a particular privacy incident will make an initial assessment on a potential or confirmed breach of PII.

The Privacy Analyst will coordinate with CSIRT to report actual breaches to the United States Computer Emergency Response Team (US-CERT).

The Privacy Analyst evaluates whether there is evidence of actual harm from a privacy breach and estimates the level of risk of PII compromise (low, moderate, or high risk). The Privacy Analyst then submits recommendations to the CPO regarding how the Agency should response to a specific privacy breach and whether notification is appropriate.

2.5 CHIEF INFORMATION SECURITY OFFICER (CISO)

The Chief Information Security Officer (CISO) is the head of Information Assurance, reporting to the CIO. The CISO administers the USAID Incident Response Program, which provides enterprise-wide management of computer security incidents in unclassified, USAID-managed network space in order to mitigate risks to USAID business operations.

The USAID Chief Information Security Officer (CISO) oversees the USAID Computer Security Incident Response Team (CSIRT), which responds to information security events that warrant further investigation, verification, and reporting. The CISO established CSIRT as the incident response and the investigative and reporting body. The CISO develops, maintains, and enforces the USAID incident response policy and procedures; serves as the focal point for the Agency cyber security incident response capability; and investigates, coordinates, and reports incidents.

The USAID incident response program provides logistical and operational support to the Privacy Office for responding to privacy incidents. For more information about the incident response program, see **ADS 545, Information Systems Security**.

2.6 COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

The Computer Security Incident Response Team (CSIRT) is responsible for administering all procedures involved in responding to incidents. CSIRT cyber threat analysts detect and analyze incidents, coordinate activities within the Office of the CIO for containing, eradicating, and recovering from cyber security incidents.

CSIRT reports cyber security and privacy incidents to US-CERT within one hour of discovery, as well as USAID CISO-CPO, appropriate system and mission Information System Security Officers, and appropriate System Owners. CSIRT establishes and implements tools and processes to ensure timely response and reporting of security incidents, monitors security tools on USAID networks, and ensures that corrective measures have been implemented.

2.7 USAID CIO SERVICE DESK

The CIO Service Desk forwards privacy incident reports to the CSIRT and the Privacy Office; and assists with incident response activities as requested by CSIRT. When requested, the CIO Service Desk disables, reconfigures, and/or removes access to systems

involved in an incident. The CIO Service Desk also establishes and implements tools and processes to ensure timely reporting of privacy incidents to CSIRT.

2.8 USAID EMPLOYEES

USAID employees must comply with the requirements of the Privacy Act and other federal privacy authorities, which require employees to report breaches of PII and to assist with all privacy breach assessment, response, and notification activities.

All employees must report immediately upon discovery all potential and actual privacy breaches to ***both*** the CIO Helpdesk at (202) 712-1234 or **CIO-HELPDESK@usaid.gov** ***and*** the Privacy Office at **privacy@usaid.gov**, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred.
For more information about an employee's responsibilities as a user of USAID PII, see **ADS 545mbd, Rules of Behavior for Users.**

3. PRIVACY BREACH NOTIFICATION

USAID employs a risk-based approach to evaluate the appropriateness and effectiveness of PII breach response activities prior to providing any external notification. USAID has established the BRT to ensure adequate consideration of the elements required to be considered prior to external breach notification.

Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require USAID to resolve a number of threshold questions. The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given.

Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the "openness principle" of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

Pursuant to OMB M-07-16, USAID will address the following elements when considering external notification:

1. **Whether breach notification is required.** When determining whether notification is required, USAID will assess the likely risk of harm caused by the privacy breach and assess the level of risk, considering the nature of the data breached; the number of individuals affected; the likelihood the PII is accessible and usable; the likelihood the privacy breach may lead to harm; and the ability of the Agency to mitigate the risk of harm.
2. **Timeliness of the notification.** When notification is appropriate, USAID will provide notification to the individuals affected without unreasonable delay.
3. **Source of the notification.** USAID will determine which USAID official will issue the

notification according to the severity of the privacy breach.

4. **Contents of the notification.** USAID will provide notification in writing, which will be concise, conspicuous, and in plain language.
5. **Means of providing the notification.** USAID will determine the most appropriate means of providing notification, considering the following types of means: Telephone; First-Class Mail; E-Mail; Existing Government Wide Services; Newspapers or other Public Media Outlets; Substitute Notice; and Accommodations.
6. **Who receives notification.** USAID will determine whether law enforcement or national security reasons will delay or debar public outreach in response to a breach. When there are not restrictions to public notification, USAID will provide prompt notification to the individuals affected. USAID will also consider notifying other persons, including the media, other federal agencies, private sector agencies, and/or the general public. USAID will provide appropriate information the General Accountability Office and Congress, when requested. When all factors have been evaluated, USAID will reassess the level of impact assigned to the PII breached and apply that reassessment to the types of notification to be provided.

4. APPENDICES

4.1 APPENDIX A DEFINITIONS

This section describes selected terms used in this document.

Access means the ability or opportunity to gain knowledge of personally identifiable information.

Breach is used to include the 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 an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Harm means damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

Incident means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of personally identifiable information, whether in electronic or paper format.

Individual means a citizen of the United States or an alien lawfully admitted for permanent residence.

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. 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, mother's

maiden name, etc. 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. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Risk means the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment means the process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system. Part of risk management and synonymous with risk analysis, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by established or planned security controls.

4.2 APPENDIX B REFERENCES

This section lists those references which provide statutes, regulations, and guidance relevant to this document.

Statutes

Freedom of Information Act of 1966 (FOIA), as amended at 5 USC 552

Privacy Act of 1974 (PA), as amended at 5 USC 552a

Paperwork Reduction Act of 1995 (PRA), as amended at 44 USC 3501-3521

Information Technology Management Reform Act of 1996 (ITMRA), known as the Clinger-Cohen Act, as amended at 40 USC 11101 and 11103

Federal Information Security Management Act of 2002 (FISMA), as amended at 44 USC 3541-3549

E-Government Act of 2002, as amended at 44 USC 3501 note § 208

Consolidated Appropriations Act, 2005, as amended at 42 USC 2000ee-2

Executive Orders and Other Presidential Documents

Executive Order (EO) 13402, Strengthening Federal Efforts to Protect Against Identity Theft (as amended, November 3, 2006)

OMB Policies

M-05-08, Designation of Senior Agency Officials for Privacy (Feb. 11, 2005)

M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)

M-06-16, Protection of Sensitive Agency Information (June 23, 2006)

M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)

OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)

M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)

NIST Guidance

NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide (August 2012)

NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010)

USAID Policies

ADS 508, USAID Privacy Policy

ADS 545, Information Systems Security

508mai_030714