Privacy Impact Assessment (PIA) Process & Procedures

A Mandatory Reference for ADS Chapter 508

New Reference Date: 08/31/2007
Responsible Office: M/CIO
File Name: 508mac_083107_cd49

Privacy Impact Assessment (PIA) Processes and Procedures

1. INTRODUCTION

Effective date: 08/31/2007

This document defines the manner in which privacy impact assessments must be conducted at USAID.

2. PRIVACY IMPACT ASSESSMENT (PIA)

Effective date: 08/31/2007

The preliminary Information Collection Checklist, that is completed for all USAID systems by the System Owners, helps the Privacy Office determine if additional processes may apply to the system.

The Information Collection Checklist, Attachment A in this document, is available on the USAID Privacy Page, **http://www.usaid.gov/pp.html**. Completed Checklists must be sent to the Privacy Office at **privacy@usaid.gov**.

2.1 When to conduct a PIA

Effective date: 08/31/2007

System Owners must conduct or update a PIA under the following circumstances:

a. For every electronic information system and information collection system (Privacy Office staff will assist System Owners in this process.);

b. Before developing or procuring IT systems, or prior to initiating a new electronic collection of information for ten or more persons (excluding agencies or employees of the Federal Government);

c. When a system change creates a new privacy risk;

d. When information collection authorities, business processes, or other factors affecting the collection and handling of PII change;

e. Every three years for existing systems without changes.

Examples of system changes that require a new PIA and/or a system Certification and Accreditation (C&A) to be conducted include the following:

a. Conversions - converting paper-based records to electronic systems;

b. Anonymous to Non-Anonymous - applying functions to an existing information collection that change anonymous information into PII;

c. Significant System Management Changes - use of relational database technologies or Web-based processing with existing PII systems to access multiple data stores;

d. Significant Data Merging - merging, centralizing, or matching databases containing PII with other databases to create one central source of information;

e. New Public Access - applying user-authenticating technology (e.g., password, digital certificate) to a publicly accessible information system;

f. Commercial Sources - incorporating purchased or commercially obtained PII into existing USAID databases;

g. New Interagency Uses - interagency initiatives that share functions or exchange PII, for example shared HSPD-12 systems and processes;

h. Internal Flow or Collection - business process changes that result in new uses or disclosures of PII;

i. Alteration in Character of Data - adding new PII, such as health or financial information, to a collection that raises risk to personal privacy.

PIAs must be reviewed by Privacy Office staff prior to permitting the system to operate in the production environment. After Privacy Office staff review and clear a PIA, they must publish the PIA on USAID's public Web site.

The Chief Privacy Officer (CPO) must report annually on all PIAs conducted on Agency systems, including legacy systems that have not had PIAs conducted as part of prior FISMA or OMB reporting.

2.2 PIA Process

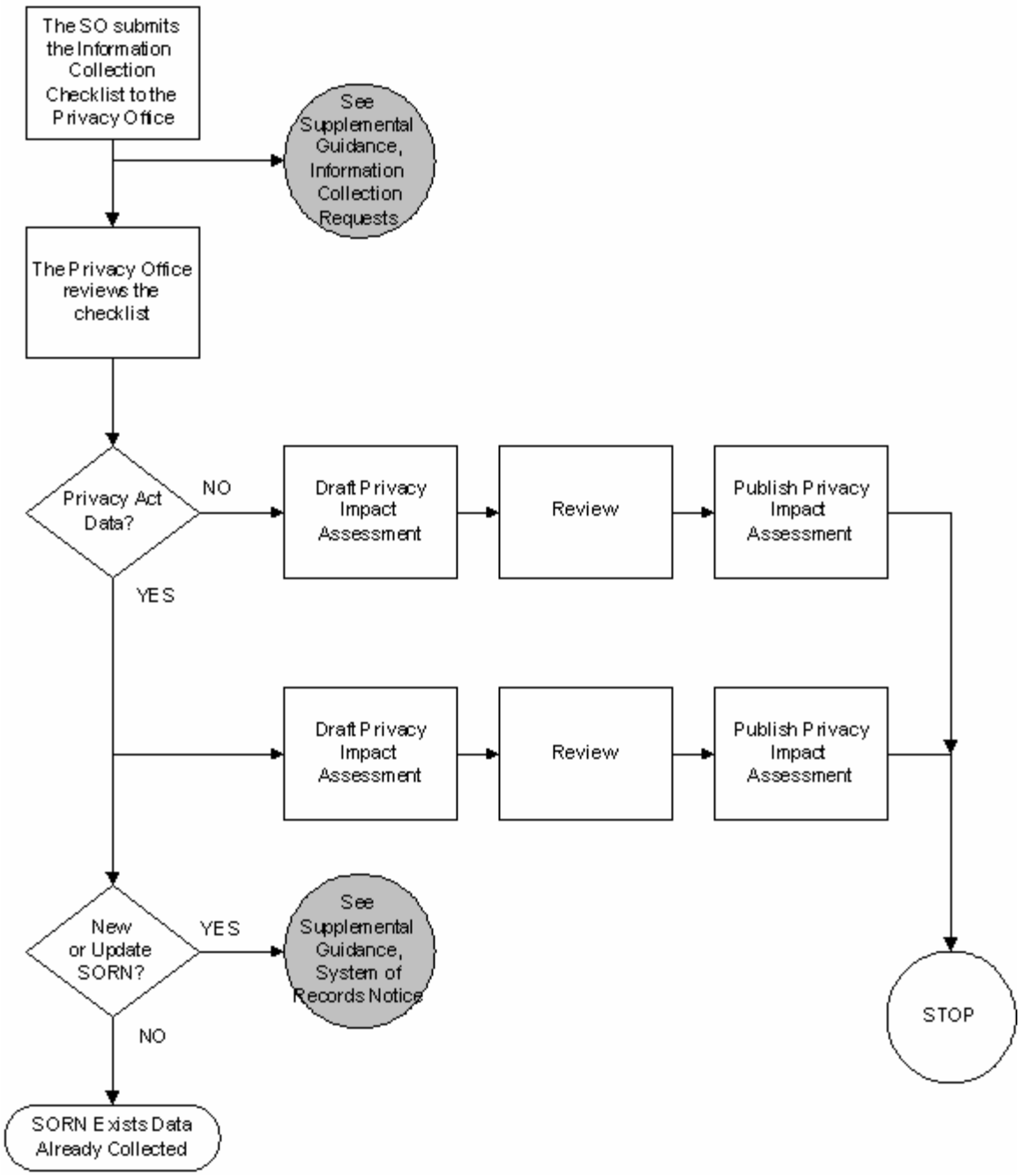
Effective date: 08/31/2007

The Privacy Impact Assessment process is a collaboration between System Owners and Privacy Office staff. The Privacy Office staff assist System Owners to furnish the necessary information and to advise them of related forms, processes, and timelines associated with conducting PIAs.

Figure 2.2, *The PIA Process*, graphically depicts the mandatory steps in the preparation and completion of a PIA.

Figure 2.2

The Privacy Impact Assessment (PIA) Process



Step 1: The System Owner completes and submits the Information Collection Checklist to the Privacy Office.

Step 2: The Privacy Office reviews the Checklist to determine if 1) the system contains PII, 2) the system is an information collection request containing PII, and 3) the system is a system of record and requires a system of record notice (SORN) to be filed with the Federal Register. Each of the decision diamonds in Figure 2.2 indicate possible progression to separate, but related processes. Separate processes are indicated by a grayed-out circle that contains the name of the supplementary guidance that describes the processes in detail.

Step 3: If the Checklist indicates that no PII is contained in the system, the Privacy Office posts a Privacy Impact Statement on the USAID Privacy Page. The statement identifies the system as one that has been examined for PII and was determined to contain none.

Step 4: If the Checklist indicates that PII is contained in the system, the Privacy Office notifies the System Owner that a full PIA must be conducted.

Step 5: The System Owner conducts the PIA and submits the completed PIA to the Privacy Office. (The System Owner may collaborate with Privacy Staff to properly complete the PIA.)

Step 6: The Privacy Office Staff reviews the PIA and prepares a recommendation/approval letter for the Chief Privacy Officer's (CPO) signature.

Step 7: After the CPO approves the PIA, Privacy Office Staff publish the PIA on the USAID Privacy Page, which is accessible by the public.

508mac_083107_w092607_cd49

ATTACHMENT A

USAID Information Collection Checklist

Instructions:
Please respond to each question by entering an "X" in the appropriate column.
For questions 1-7, "how many" may be estimated.
Return completed forms via e-mail to privacy@usaid.gov.

	Who are you collecting from?	YES	NO	How Many?
1	Are you requesting information from USAID Direct Hire Staff?			
2	Are you requesting information from USAID Contractors (includes IC's and PSC's)?			
3	Are you requesting information from other Federal Agencies?			
4	Are you requesting information from State, local or tribal Governments?			
5	Are you requesting information from small businesses, educational, or non-profit institutions?			
6	Are you requesting information from the public (US citizens or legal permanent residents)?			
7	Are you requesting information from non-US citizens?			
	What are you collecting?	YES	NO	
8	Will the system contain the any of the following, which are personally identifiable information?			
8(a)	Name			
8(b)	Social Security Number			
8(c)	Date of Birth			
8(d)	Place of Birth			
8(e)	Mother's Maiden Name			
8(f)	Biometric Records (fingerprint, photograph, voice print, etc.)			
8(g)	Educational Records (transcripts, conduct reports, etc.)			
8(h)	Financial Records			
8(i)	Medical History			
8(j)	Criminal History			
8(k)	Employment History			
	How are you collecting it?	YES	NO	
9	Will the collection be manual or paper-based?			
10	Will the collection be electronic (server, e-mail, web-based, etc.)?			
11	Will the records be retrieved by any data element in item 8(a) - 8(k) above?			
12	What is the purpose for the collection of this information?			
13	How is this information going to be used after it is collected?			
14	Who will have access to the information?			