



USAID
FROM THE AMERICAN PEOPLE

AFR Interns Database Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
AFR Interns Database
Approved Date: November 10, 2015

Additional Privacy Compliance Documentation Required:

- None
- System of Records Notice (SORN)
- Open Data Privacy Analysis (ODPA)
- Privacy Act Section (e)(3) Statement or Notice (PA Notice)
- USAID Web Site Privacy Policy
- Privacy Protection Language in Contracts and Other Acquisition-Related Documents
- Role-Based Privacy Training Confirmation

Possible Additional Compliance Documentation Required:

- USAID Forms Management. [ADS 505](#)
- Information Collection Request (ICR). [ADS 505](#), [ADS 506](#), and [ADS 508 Privacy Program](#)
- Records Schedule Approved by the National Archives and Records Administration. [ADS 502](#)

Table of Contents

<i>1</i>	<i>Introduction</i>	<i>1</i>
<i>2</i>	<i>Information</i>	<i>1</i>
2.1	Program and System Information.....	1
2.2	Information Collection, Use, Maintenance, and Dissemination.....	4
<i>3</i>	<i>Privacy Risks and Controls</i>	<i>6</i>
3.1	Authority and Purpose (AP).....	6
3.2	Accountability, Audit, and Risk Management (AR).....	7
3.3	Data Quality and Integrity (DI).....	8
3.4	Data Minimization and Retention (DM).....	8
3.5	Individual Participation and Redress (IP).....	9
3.7	Transparency (TR).....	9
3.8	Use Limitation (UL).....	10
3.9	Third-Party Web Sites and Applications.....	11

1 Introduction

The USAID Privacy Office is using this Privacy Impact Assessment (PIA) Template to gather information from program managers, system owners, and information system security officers in order to analyze USAID information technology and information collections (systems) that collect, use, maintain, or disseminate personally identifiable information (PII). See [ADS 508 Privacy Program](#) Section 503.3.5.2 Privacy Impact Assessments.

2 Information

2.1 Program and System Information

2.1.1 Describe the PROGRAM and its PURPOSE.

In sub-Saharan Africa, USAID works to help build sustained and well-governed states that respond to the needs of their people, reduce widespread poverty, and conduct themselves responsibly in the international system. Our assistance to Africa aims to help African governments, institutions, and organizations advance good governance principles and innovative approaches to health, education, economic growth, agriculture, and the environment.

The summer intern program exposes American citizens to international development and promotes cross-cultural understanding while providing student with an opportunity to experience work with USAID. Interns will have the opportunity to contribute to USAID's work in Africa while learning valuable lessons about international development and working closely with our staff members. The work assigned to an intern in most office divisions includes research, writing program memoranda, drafting documents, facilitating meetings and special events, attending program discussions in the Agency and at the Department of State, and communicating on program issues for USAID field Missions abroad. This is an excellent opportunity for outstanding students interested in pursuing careers in international development.

2.1.2 Describe the SYSTEM and its PURPOSE.

USAID's Africa Bureau hosts a limited number of summer interns in some of our overseas missions in sub-Saharan Africa as well as in Washington, D.C. Students apply online at the USAID web site through an applicant database developed by M/CIO for Africa Bureau several years ago. The online application form asks for basic information as well as a description of foreign language skills and overseas experience. Student applicants are also asked to submit a statement of intent, and resume (or CV) online. The statement of intent discusses the students' interest in development and indicates how the internship fits into their career goals. The application is open for applications for a limited timeframe, usually 2 months (November-December). After submitting an application, student applicants receive an email with a confirmation notice and a unique code. Professors will use this code to access the application site and upload their letters of recommendation directly, without being able to view the application. The application is administered by AFR/DP in collaboration with CIO. AFR/DP director is the only administrator who controls access to view applications through an individually granted password protected login system.

2.1.3 What is the SYSTEM STATUS?

- New System Development or Procurement
- Pilot Project for New System Development or Procurement
- Existing System Being Updated
- Existing Information Collection Form or Survey
OMB Control Number:
- New Information Collection Form or Survey
- Request for Dataset to be Published on an External Website
- Other:

2.1.4 What types of INFORMATION FORMATS are involved with the program?

- Physical only
- Electronic only
- Physical and electronic combined

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

- No.
- Yes:
 - Information Collection Forms or Surveys
 - Third Party Web Site or Application
 - Collaboration Tool

2.1.6 What type of system and/or TECHNOLOGY is involved?

- Infrastructure System (Local Area Network, Wide Area Network, General Support System, etc.)
- Network
- Database
- Software
- Hardware
- Mobile Application or Platform
- Mobile Device Hardware (cameras, microphones, etc.)
- Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
- Wireless Network

2.1.6 What type of system and/or TECHNOLOGY is involved?
<input type="checkbox"/> Social Media
<input type="checkbox"/> Web Site or Application Used for Collaboration with the Public
<input type="checkbox"/> Advertising Platform
<input type="checkbox"/> Website or Webserver
<input type="checkbox"/> Web Application
<input type="checkbox"/> Third-Party Website or Application
<input type="checkbox"/> Geotagging (locational data embedded in photos and videos)
<input type="checkbox"/> Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)
<input type="checkbox"/> Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)
<input type="checkbox"/> Facial Recognition
<input type="checkbox"/> Identity Authentication and Management
<input type="checkbox"/> Smart Grid
<input type="checkbox"/> Biometric Devices
<input type="checkbox"/> Bring Your Own Device (BYOD)
<input type="checkbox"/> Remote, Shared Data Storage and Processing (cloud computing services)
<input checked="" type="checkbox"/> Other: CIO designed database on USAID.gov
<input type="checkbox"/> None

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
<input checked="" type="checkbox"/> Citizens of the United States
<input type="checkbox"/> Aliens lawfully admitted to the United States for permanent residence
<input type="checkbox"/> USAID employees and personal services contractors
<input type="checkbox"/> Employees of USAID contractors and/or services providers
<input type="checkbox"/> Aliens
<input type="checkbox"/> Business Owners or Executives
<input type="checkbox"/> Others:
<input type="checkbox"/> None

2.2 Information Collection, Use, Maintenance, and Dissemination

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
<input checked="" type="checkbox"/> Name, Former Name, or Alias
<input type="checkbox"/> Mother's Maiden Name
<input type="checkbox"/> Social Security Number or Truncated SSN
<input type="checkbox"/> Date of Birth
<input type="checkbox"/> Place of Birth
<input checked="" type="checkbox"/> Home Address
<input type="checkbox"/> Home Phone Number
<input checked="" type="checkbox"/> Personal Cell Phone Number
<input checked="" type="checkbox"/> Personal E-Mail Address
<input type="checkbox"/> Work Phone Number
<input type="checkbox"/> Work E-Mail Address
<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Passport Number or Green Card Number
<input type="checkbox"/> Employee Number or Other Employee Identifier
<input type="checkbox"/> Tax Identification Number
<input type="checkbox"/> Credit Card Number or Other Financial Account Number
<input type="checkbox"/> Patient Identification Number
<input type="checkbox"/> Employment or Salary Record
<input type="checkbox"/> Medical Record
<input type="checkbox"/> Criminal Record
<input type="checkbox"/> Military Record
<input type="checkbox"/> Financial Record
<input checked="" type="checkbox"/> Education Record
<input type="checkbox"/> Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
<input checked="" type="checkbox"/> Sex or Gender
<input type="checkbox"/> Age

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?

- Other Physical Characteristic (eye color, hair color, height, tattoo)
- Sexual Orientation
- Marital status or Family Information
- Race or Ethnicity
- Religion
- Citizenship
- Other: Current year in college (Freshman, Sophomore, etc.)
- No PII is collected, used, maintained, or disseminated

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?

- Log Data (IP address, time, date, referrer site, browser type)
- Tracking Data (single- or multi-session cookies, beacons)
- Form Data
- User Names
- Passwords
- Unique Device Identifier
- Location or GPS Data
- Camera Controls (photo, video, videoconference)
- Microphone Controls
- Other Hardware or Software Controls
- Photo Data
- Audio or Sound Data
- Other Device Sensor Controls or Data
- On/Off Status and Controls
- Cell Tower Records (logs, user location, time, date)
- Data Collected by Apps (itemize)
- Contact List and Directories
- Biometric Data or Related Data

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?

- SD Card or Other Stored Data
- Network Status
- Network Communications Data
- Device Settings or Preferences (security, sharing, status)
- Other: Once information is entered the form is submitted.
- None

2.2.4 Who owns and/or controls the system involved?

- USAID Office: AFR/DP in collaboration with M/CIO
- Another Federal Agency:
- Contractor:
- Cloud Computing Services Provider:
- Third-Party Website or Application Services Provider:
- Mobile Services Provider:
- Digital Collaboration Tools or Services Provider:
- Other:

3 Privacy Risks and Controls

3.1 Authority and Purpose (AP)

3.1.1 What are the statutes or other LEGAL AUTHORITIES that permit you to collect, use, maintain, or disseminate personal information?

5 U.S.C. 301; Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.

e-Government Act of 2002 (H.R. 2458/S.803) supports government to government services.

<http://www.whitehouse.gov/omb/egov/g-4-act.html>

3.1.2 Why is the PII collected and how do you use it?

The PII is collected on an application form in order to identify applicants applying for an internship and be able to verify that they are in fact students who are eligible U.S. citizens. Email/phone is used to contact them about their application. No personal information (other than the email address) is utilized outside the password protected system.

3.1.3 How will you identify and evaluate any possible new uses of the PII?

There is no intention to ever use information after the application period has passed. All logins except the System Administrator are deleted from the system annually to avoid unauthorized access.

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

No:

Yes:

Form or Survey (Please attach)

OMB Number, if applicable:

Privacy Act Statement (Please provide link or attach PA Statement)

3.2.3 Who owns and/or controls the personal information?

USAID Office: AFR/DP Only

Another Federal Agency:

Contractor:

Cloud Computing Services Provider:

Third-Party Web Services Provider:

Mobile Services Provider:

Digital Collaboration Tools or Services Provider:

Other:

3.2.8 Do you collect PII for an exclusively statistical purpose? If you do, how do you ensure that the PII is not disclosed or used inappropriately?

No.

Yes:

3.3 Data Quality and Integrity (DI)

3.3.1 How do you ensure that you collect PII to the greatest extent possible directly from the subject individual?

The individual receives a unique login to control access.

3.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?

Information is provided directly from the source individuals.

3.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?

N/A. There are new applicants every year.

3.4 Data Minimization and Retention (DM)

3.4.1 What is the minimum PII relevant and necessary to accomplish the legal purpose of the program?

The PII is collected on an application form in order to identify applicants applying for an internship and be able to verify that they are in fact students who are eligible U.S. citizens. Email/phone is used to contact them about their application. No personal information (other than the email address) is utilized outside the password protected system.

3.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

No.

Yes:

3.4.4 What types of reports about individuals can you produce from the system?

The data can be exported to a spreadsheet. It is not for distribution but only to aid field missions and Washington offices in sorting through applications. Making the data anonymized would render it useless for the purpose of interviewing/selecting a specific intern.

3.4.6 Does the system monitor or track individuals?

(If you choose Yes, please explain the monitoring capability.)

No.

Yes: Only in terms of last logon to the system, which is available only to the AFR/DP administrator through a report function.

3.5 Individual Participation and Redress (IP)**3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?**

It is implicit since they voluntarily fill out the form with their data to apply for the internship.

3.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

Students can email the system administrator to modify data once an application is submitted.

3.5.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that the PII will be available to individuals who request access to and amendment of their PII?

N/A

3.7 Transparency (TR)**3.7.1 Do you retrieve information by personal identifiers, such as name or number?**

(If you choose Yes, please provide the types of personal identifiers that are used.)

No.

Yes: Data can be searched based on any data field in the system provided by applicants.

3.7.2 How do you provide notice to individuals regarding?

3.7.2 How do you provide notice to individuals regarding?

- 1) The authority to collect PII:
- 2) The principal purposes for which the PII will be used:
- 3) The routine uses of the PII:
- 4) The effects on the individual, if any, of not providing all or any part of the PII:

Privacy Notice

USAID will only use your personal information for the purpose for which it was provided, such as to review your application during the selection process. When you voluntarily submit information, it constitutes your consent to the use of the information for the purpose stated. When you click the "Submit" button on any of the Web forms found on our sites, you are indicating your voluntary consent to the use of the information you submit, for the stated purpose.

We would like to make you aware of a law that provides to you with certain rights concerning your personal information. This is described in the Privacy Act of 1974 (as amended by 5 U.S.C. 552a) governing Federal Records. This law concerns any information held in a Privacy Act System of Records (SOR) that can be retrieved by a personal identifier such as name, social security number, or other identifying number or symbol. An individual is entitled to access to his or her records and to request correction of these records if applicable. The Privacy Act prohibits disclosure of these records without the written consent of the individual(s) to whom the records pertain unless one of the twelve disclosure exceptions enumerated in the Act applies. The actual Act can be found at this link: <http://www.justice.gov/opcl/privstat.htm>.

3.7.3 Is there a Privacy Act System of Records Notice (SORN) that covers this system?

- No
- Yes: OPM GOV-1, General Personnel Records, 77 FR 73694 (Dec. 11, 2012); and OPM GOV-5, Recruiting, Examining and Placement, 71 FR 35342, 35350 (June 19, 2016)

3.7.4 If your system involves cloud computing services, how do you ensure that you know the location of the PII and that the SORN System Location(s) section provides appropriate notice of the PII location?

N/A

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

Only those within the Bureau granted logins, only for the duration of the application period after which all logins are deleted except the system administrator .

3.8.3 With whom do you share the PII outside of USAID? And whether (and how, if applicable) you will be using the system or related web site or application to engage with the public?

Not shared.

**3.8.4 Do you share PII outside of USAID?
If so, how do you ensure the protection of the PII 1) as it moves from USAID to the outside entity and 2) when it is used, maintained, or disseminated by the outside entity?**

No.

Yes:

3.9 Third-Party Web Sites and Applications

3.9.1 What PII *could be made available* (even though not requested) to USAID or its contractors and service providers when engaging with the public?

N/A

Appendix A. Links and Artifacts

A.1 Privacy Compliance Documents or Links
<input type="checkbox"/> None. There are no documents or links that I need to provide.
<input type="checkbox"/> Privacy Threshold Analysis (PTA)
<input type="checkbox"/> Privacy Impact Assessment (PIA)
<input type="checkbox"/> System of Records Notice (SORN)
<input type="checkbox"/> Open Data Privacy Analysis for Posting Datasets to the Public (ODPA)
<input type="checkbox"/> Data Collection Forms or Surveys
<input type="checkbox"/> Privacy Act Section (e)(3) Statements or Notices
<input type="checkbox"/> USAID Web Site Privacy Policy
<input type="checkbox"/> Privacy Policy of Third-Party Web Site or Application
<input type="checkbox"/> Privacy Protection Language in Contracts and Other Acquisition-Related Documents