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

PRIVACY IMPACT ASSESSMENT (PIA)

Program Name: Bureau for Legislative and Public Affairs Public Information Production and Online Services

System Name: Social Media including Facebook, Flickr, GitHub, Instagram, LinkedIn, Storify, Twitter, Tumblr, and YouTube

Version 1F

Approved: May 6, 2014

TABLE OF CONTENTS

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.

The PIA process should accomplish two goals: 1) determine the privacy risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate and enforce protections and alternative processes for handling PII to reduce potential privacy risks to acceptable levels.

Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable. Each section includes assistance (in blue text) on how to answer the question. For additional instructions on how to complete this PIA Template, please see Appendix C Conducting the PIA.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at privacy@usaid.gov.

2. CONTACT INFORMATION AND APPROVAL SIGNATURES

3. COMPLIANCE REQUIREMENTS

3.1 PRIVACY REQUIREMENTS

3.1.1 Privacy Compliance Requirements *(The following additional privacy compliance actions and/or documents are required for this system.)*
☒ Privacy Impact Assessment (PIA). See ADS 508 Privacy Program Section 503.3.5.2 and PIA Template
☒ System of Records Notice (SORN). See ADS 508 Privacy Program Section 503.3.10.2 and SORN Template
☐ Open Data Privacy Analysis for Posting Datasets to the Public (ODPA). See ADS 508 Privacy Program Section 503.3.11.1 and ODPA Template
☐ Privacy Act Section (e)(3) Statement or Notice on Surveys and Forms (Privacy Statement or Notice). See ADS 508 Privacy Program Section 503.3.10.1 and Guidance for Privacy Statements or Notices
☒ USAID Web Site Privacy Policy. See ADS 508 Privacy Program Section 503.3.10.4 and USAID Web Site Privacy Policies Requirements
☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents. See ADS 508 Privacy Program Sections 503.3.5.3, 3.5.4, and 3.5.5
☐ Role-Based Privacy Training Confirmation. See ADS 508 Privacy Program Section 503.3.5.8
☐ None

3.2 POSSIBLE ADDITIONAL COMPLIANCE REQUIREMENTS

3.2.1 Compliance Requirements *(The following additional privacy compliance actions and/or documents are required for this system.)*
☐ USAID Forms Management, contact USAID Information and Records Division (M/MS/IRD). See ADS 505
☐ Information Collection Request (ICR), contact USAID Information and Records Division (M/MS/IRD). See ADS 505 and ADS 506, as well as ADS 508 Privacy Program Section 503.3.10.1 and Guidance for Privacy Statements or Notices
☒ Records Schedule Approved by the National Archives and Records Administration, contact USAID Information and Records Division (M/MS/IRD). See ADS 502

☐ None

4. PTA INFORMATION

4.1 PROGRAM INFORMATION

4.1.1 Describe the program and its purpose.

Social media networking interactions and applications includes a sphere of non-government web sites and web-based tools that focus on connecting users, inside and outside of USAID. Social media is used to engage in dialogue, share information and media, and collaborate. Third-parties control and operate these non-governmental websites; however, USAID may use them as alternative channels to provide robust information and to engage with the public. USAID may also use these web sites to make information and services widely available, while promoting transparency and accountability, as a service for those seeking information about, collaboration with, or services from USAID.

In light of the vast capabilities of social media web services, USAID leverages these applications in order to enhance USAID's ability to communicate with the public, as well as increase government transparency and promote public participation and collaboration through a more efficient, streamlined process of information dissemination to the public. USAID has created official accounts on the several social media web services listed on the title page. The USAID official accounts on these social media web services will be used as a mechanism to provide mission-related information to the public. The USAID Bureau of Legislative and Public Affairs (LPA) will be the primary account holder of USAID's accounts on these social media web sites. As such, LPA will be responsible for ensuring that information posted to these web sites is appropriate and approved for public dissemination.

Provide a general description of the program. The description should include the purpose of the program and how it supports a USAID business function. Describe the way the program operates to achieve its purpose, and any interconnections with other programs. Provide information on where the program operates, such as locally, stateside, overseas, or worldwide. The description should be as comprehensive as necessary to assist the public in understanding the program fully.

Describe the types of information that you use, and explain why you use the information. The description should show who uses the information, how the information moves within the program, how information is transmitted to and from the program, and how the information is stored. The description should be as comprehensive as necessary to assist the public in understanding fully the ways and means information flows as the program functions.

AP-2 Purpose Specification

4.1.2 What types of information formats are involved with the program?

(Please check all that apply.)

☐ Physical only

☒ Electronic only

☐ Physical and electronic combined

Physical formats include paper documents, spreadsheets, and photos; cards; passports; and computer print outs.

Electronic formats include IT systems, electronic media (CDs, thumb drives), digital collaboration tools or services, mobile services, video and audio records, biometric scans, and electronic images.

For this purpose, *system* means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange,

transmission, or reception of data or information.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

SE-1 Inventory of Personally Identifiable Information

4.1.3 Does your program engage with the public?

☐ No.

☒ Yes:

☐ Information Collection Forms or Surveys

☒ Third Party Web Site or Application

☒ Collaboration Tool

The use of third-party websites and applications, digital collaboration services, and other new technologies can increase privacy risks, because these technologies can make PII available to USAID even when USAID does not purposefully collect it.

DM-1 Minimization of Personally Identifiable Information

4.1.4 Do you retrieve information by personal identifiers, such as name or number?

USAID does not retrieve information by personal identifiers through its social media platforms. Instead, users find USAID through search features, hashtags, etc., and follow, like, subscribe to see the Agency's information.

When using social media, USAID will use hashtags (#) and the at sign @ to tag keywords (such as #endpoverty), principals (such as @rajshah) in posts to make our content more easily searchable and transparent.

Describe how you retrieve information from where you store it. Describe whether you retrieve information by **name** of the individual or by some **identifying number, symbol, or other identifying particular**, provide a detailed description of the identifiers or retrieval elements.

You might store paper forms in a filing cabinet and retrieve them by name of the person who submitted the form or by date of submission. The name would be a personal identifier, but the date of submission would not. You might search a database using the name of the country where USAID is supporting several projects. The country name would not be a personal identifier.

TR-2 System of Records Notices and Privacy Act Statements

4.1.5 Do you have privacy compliance documents for this system? *(Please check all that apply and attach documents. If you choose* Other*, please provide a copy of or link to the documents in Appendix D to this PTA.)*
☐ Information Collection Checklist (ICC) (no longer used; replaced by PTA)
☐ Privacy Threshold Analysis (PTA)
☐ Privacy Impact Assessment (PIA)
☐ Open Data Privacy Analysis for Posting Datasets to the Public (ODPA)
☐ Privacy Act Section (e)(3) Statement or Notice on Surveys and Forms (Privacy Statement or Notice)
☒ Web Site Privacy Policy: USAID Web Site Privacy Policy
☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents
☐ Role-Based Privacy Training Confirmation
☐ Others:

4.2 INFORMATION COLLECTION, USE, MAINTENANCE, AND DISSEMINATION

4.2.1 What types of personal information do you collect, use, maintain, or disseminate? *(Please check all that apply. If you choose* Other*, please list the additional types of PII.)*
☒ Name, Former Name, or Alias: USAID does not collect names, but may disseminate names of subjects of photos in hashtags, etc.
☐ Mother's Maiden Name
☐ Social Security Number or Truncated SSN
☐ Date of Birth
☐ Place of Birth
☐ Home Address
☐ Home Phone Number
☐ Personal Cell Phone Number
☐ Personal E-Mail Address
☐ Work Phone Number
☐ Work E-Mail Address
☐ Driver's License Number
☐ Passport Number or Green Card Number

☐ Employee Number or Other Employee Identifier
☐ Tax Identification Number
☐ Credit Card Number or Other Financial Account Number
☐ Patient Identification Number
☐ Employment or Salary Record
☐ Medical Record
☐ Criminal Record
☐ Military Record
☐ Financial Record
☐ Education Record
☒ Biometric Record (signature, fingerprint, photograph, voice print, physical movement, DNA marker, retinal scan, etc.): photos, video, sound recordings.
☐ Sex or Gender
☐ Age
☐ Other Physical Characteristic (eye color, hair color, height, tattoo)
☐ Sexual Orientation
☐ Marital status or Family Information
☐ Race or Ethnicity
☐ Religion
☐ Citizenship
☒ Other: Hashtags of broad geographic locations of photos, such as country.
☐ None
SE-1 Inventory of Personally Identifiable Information

4.2.2 About what types of people do you collect, use, maintain, or disseminate personal information?
(Please check all that apply. If you choose Other*, please provide the types of people.)*
☒ Citizens of the United States
☒ Aliens lawfully admitted to the United States for permanent residence
☒ USAID employees and personal services contractors

☒ Employees of USAID contractors and/or services providers
☒ Aliens
☒ Business Owners or Executives
☐ Others:
AP-1 Authority to Collect

4.2.3 What types of digital or mobile data do you collect, use, maintain, or disseminate? *(Please check all that apply. If you choose* Other*, please provide the types of data.)*
☐ 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: Hashtags of broad geographic location of photos, such as country. No geotagging at this time. See PIA Sections 4.2.1, 5.1.2, 5.2.8, 5.4.1, and 5.6.1.
☐ Camera Controls (photo, video)
☐ 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): “friends”, “likes”, “followers”, “favorite”, “subscribe”, “connect”
☐ Contact List and Directories
☐ Biometric Data or Related Data
☐ SD Card or Other Stored Data
☐ Network Status

☐ Network Communications Data
☐ Device Settings or Preferences (security, sharing, status)
☐ Other:
☐ None
AR-2 Privacy Impact and Risk Assessment SE-1 Inventory of Personally Identifiable Information

4.2.4 What are the statutes or other legal authorities that permit you to collect, use, maintain, or disseminate personal information?

5 USC 301, Departmental Regulations; 22 U.S.C. Ch. 32, Subchapter I, Foreign Assistance Act of 1961, as amended.
Please provide the name and citation for each statute, regulation, policy, and other authority (such as Executive Orders, OMB policies, NIST guidance) that authorize you to collect, use, maintain, and disseminate PII. Also include any Memoranda of Understanding (MOUs) that allow or require you to collect, use, maintain, and/or disseminate PII. Include also any internal USAID regulations, policies, memoranda, and other documents. Regarding Social Security Numbers (SSNs), please provide the name and citation for each statute, regulation, policy, and other authority that authorizes you to collect, use, maintain, and disseminate SSNs, if you do so. Describe how these authorities define the collection, use, maintenance, and dissemination of the PII or SSNs and relate to the program and system purpose.
AP-1 Authority to Collect

4.2.5 Who owns and/or controls the personal information?

(Please check all that apply. Please provide the names of the specific organizations. If you choose Other, *please provide the types of organizations and the name of each organization.)*

☒ USAID Office:
☐ Another Federal Agency:
☐ Contractor:
☐ Cloud Computing Services Provider:
☒ Third-Party Web Services Provider: See PIA Title Page
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:
AR-3 Privacy Requirements for Contractors and Service Providers UL-1 Internal Use

4.3 SYSTEM INFORMATION

4.3.1 Describe the system and its purpose.

Facebook is a social network that allows users to share content with their friends and fans. USAID uses Facebook pages to reach audiences who might have an interest in our work, but are not necessarily a part of the international development community. On our Facebook page we tell the story of USAID through links to blog items, our website, photos, and video. In accordance with the President's Memorandum on Transparency and Open Government and the Open Government Directive (2009), USAID uses Facebook to further engage the public. LPA promotes transparency by making information about the U.S. role in international development and disaster assistance widely available to the general public through our Facebook page.

Flickr is a photo and video hosting website and mobile application used to share and embed photos and videos. It is also used by photo researchers and by bloggers to host images that they embed in blogs and social media. The public can access photos and videos from Flickr without the need to register an account. However, users must create an account in order to upload content onto the website, to create a profile page containing photos and videos that the user has uploaded, and to gain the ability to add another Flickr user as a contact.

GitHub is a U.S. owned web-based hosting service for software development projects that uses the Git revision control system for collaborative development of software. Git is a source code revision management and development system that allows distributed programmers to perform software updates and modifications. Software developed using GitHub is open source software (OSS), which is openly available software that can be freely modified and redistributed. OSS, particularly when combined with an editing system such as Git and a popular hosting site such as GitHub, can have a number of important advantages over traditional means of software development in terms of quality, cost, and development cycle time, including: Review of software code, updates and edits by a broad range of programmers, thereby improving software function and reliability; thorough and rapid testing and debugging; and timely updates, allowing the software to continually meet user needs and remain current with prevailing trends. Under the Digital Government Strategy, USAID is required to set up a developer hub at www.usaid.gov/developer. As suggested, USAID will include on its /developer pages a link to a code repository, specifically GitHub, and create a USAID page on GitHub. GitHub is currently used by several federal agencies for the development of various software applications. GitHub is a software code repository, so any information that USAID posts will be in the form of publicly available computer code, or narrative text, much in the way that we use a social media tool like FaceBook. USAID will not be posting anything that is sensitive or not already made publically available. Information that the external community would post to the USAID GitHub site would be voluntary and can be made anonymously. USAID's use of GitHub will promote public participation and collaboration and will increase government transparency by allowing the public to directly observe and participate in the design and implementation of certain USAID software projects. This will enable the public to understand more fully the software that USAID uses. In turn, USAID will benefit from the use of GitHub by obtaining higher quality software with reduced development time and lower development costs.

Instagram is an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, including Facebook, Twitter, and Flickr. Instagram is one of the fastest growing social media applications in the world. The platform has more than 150 million users worldwide. Each day more than 55 million photos and videos are posted and shared using the platform. In total, over 16 billion photos and videos have been shared through Instagram. Instagram is particularly popular among younger audiences. The younger audiences are considered one the top audiences with whom USAID communicates. As this platform is becoming one of the largest and most effective tools to communicate visually with people, the Bureau for Legislative and Public Affairs (LPA) would like to use this as a tool to communicate the work we do. LPA's mandate is to communicate to audiences worldwide about U.S. assistance. LPA will use Instagram to share photos and videos of our assistance and the work we are doing around the world. By showing compelling photos and videos of the work USAID is doing, we can garner more support for the Agency and for the work of international development.

LinkedIn is an international social networking website for people in professional occupations with the mission to connect the world's professionals to make them more productive and successful. LinkedIn provides access to professional people and organizations, as well as related news, updates, and electronic conversations that can provide enhanced information sharing, collaboration, and horizontal communication among multiple users. In

accordance with the President's Memorandum on Transparency and Open Government and the Open Government Directive (2009), USAID will use LinkedIn to further engage the public. We will promote transparency by making information about the U.S. role in international development and disaster assistance widely available to international LinkedIn membership through our LinkedIn page.

Storify is a web site that provides a platform for users to tell stories by collecting updates from social networks, amplifying the voices that matter to create a new story format that is interactive, dynamic and social. LPA uses Storify to curate social networks to build social stories, bringing together media scattered across the Web into a coherent narrative about USAID activities. LPA searches social media networks, such as Twitter, Facebook, YouTube, Flickr, and Instagram, to find media elements about USAID.

Tumblr is a microblogging platform and social networking web site and mobile application. Tumblr allows users to post multimedia and other content to a short-form blog on a dashboard. Users can follow other users' blogs, as well as make their blogs private. The dashboard a live feed of recent posts from blogs that they follow. Through the dashboard, users are able to comment, reblog, and like posts from other blogs that appear on their dashboard. The dashboard allows the user to upload text posts, images, video, quotes, or links to their blog. Users are also able to connect their blogs to their Twitter and Facebook accounts, so whenever they make a post, it will also be sent as a tweet and a status update. Users are also able to set up a schedule to delay posts that they make and can spread their posts over several hours or even days. For each post a user creates, the user is able to help the audience find posts about certain topics by adding tags.

Twitter is a social network that allows micro blogging. Tweets are limited to 140 characters. USAID will use Twitter to disseminate mission related links and information to the public. In accordance with the President's Memorandum on Transparency and Open Government and the Open Government Directive (2009), USAID will use Twitter to further engage the public. We will promote transparency by making information about the U.S. role in international development and disaster assistance widely available to the general public through our Twitter feed.

YouTube is a social network that allows the uploading of video content. This content can then easily be shared with others by embedding in blogs, webpages, or other social media. In accordance with the President's Memorandum on Transparency and Open Government and the Open Government Directive (2009), USAID will use YouTube to further engage the public. We will promote transparency by making information about the U.S. role in international development and disaster assistance widely available to the general public through our YouTube channel.

Provide a general description of the system. The description should include the purpose of the system and how it supports the USAID program's business function. Describe the way the system operates to achieve its purpose, how information is transmitted to and from the system, and any interconnections with other systems. Describe how the system will be used at USAID and provide information on where the system will be used, such as locally, stateside, overseas, or worldwide. Provide the system level, such as major application or general support system.

Examples of other information that should be included in the description, if applicable: New technology replacing a legacy system; system is a government-wide initiative or best practice; program is moving from a paper process to IT system; or the system has interdependencies on other systems.

The description should be as comprehensive as necessary to assist the public in understanding the system fully.

For this purpose, *system* means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

AP-2 Purpose Specification

4.3.2 What type of system and/or technology is involved? *(Please check all that apply. If you choose* New Technology *or* Other*, please explain.)*
☐ 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
☒ Social Media
☒ Web Site or Application Used for Collaboration with the Public
☐ Advertising Platform
☐ Website or Webserver
☐ Web Application
☒ Third-Party Website or Application
☐ Geotagging (locational data embedded in photos and videos)
☐ Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)
☐ Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)
☐ Facial Recognition
☒ Identity Authentication and Management
☐ Smart Grid
☐ Biometric Devices
☐ Bring Your Own Device (BYOD)
☐ Remote, Shared Data Storage and Processing (cloud computing services)
☐ Other:
☐ None
AR-2 Privacy Impact and Risk Assessment

4.3.3 What is the system status? *(Please check all that apply. If you choose* Other*, please explain.)*
☒ 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:
AR-2 Privacy Impact and Risk Assessment

4.3.4 Do you use technology in ways not previously used by USAID? *(If you choose* Yes*, please provide the specifics of any new privacy risks and mitigation strategies.)*
☒ No.
☐ Yes:
Describe the new technology or the way you use technology that is new to USAID. Describe how such new technology or uses will affect the risks to the PII in the system.
AR-2 Privacy Impact and Risk Assessment

4.3.5 Who owns and/or controls the system involved? *(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)*
☒ USAID Office: Bureau for Legislative and Public Affairs
☐ Another Federal Agency:
☐ Contractor:
☐ Cloud Computing Services Provider:
☒ Third-Party Website or Application Services Provider: See PIA title page
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:
Cloud computing is remote, often shared, data storage and processing. NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a

shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (Software as a Service, Platform as a Service, Infrastructure as a Service), and four deployment models (private cloud, community cloud, public cloud, hybrid cloud). *Third-party website or application* means web-based technologies that are not exclusively operated or controlled by a government entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website.
AR-3 Privacy Requirements for Contractors and Service Providers UL-1 Internal Use

5. PRIVACY RISKS AND CONTROLS

The questions in this section focus on the specific privacy risks of your system and the mitigation strategies (controls) that help you reduce the risks of collecting, using, maintaining, and disseminating PII. The Privacy Controls focus on information privacy as a value distinct from, but interrelated with, information security. The Privacy Controls are the administrative, technical, and physical safeguards employed within USAID to protect and ensure the proper handling of PII. For more in-depth information about these Privacy Controls, please see Appendix D Privacy Controls.

5.1 AUTHORITY AND PURPOSE (AP)

The Authority and Purpose Privacy Control Family ensures that USAID identifies the legal bases that authorize a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected.

5.1.1 Why is the PII collected and how do you use it?
LPA will not collect PII from the social media members or public users and will abide by the USAID Web Site Privacy Policy. The PII collected through these social media accounts, as identified in section 4.2.1, is limited in nature and scope. Through the social media accounts, USAID will post photos, video, and sound recordings of USAID's work, which may sometimes include PII. LPA will not use geotagging at this time. The Agency will make a risk and privacy determination if and when geo-tagging will be enabled. In this circumstance the Deputy Assistant Administrator for Public Affairs will make the determination, after working with the Privacy Office to update the PIA, pursuant to ADS 508 Privacy Program Section 3.5.2, Privacy Impact Assessments.
Describe purposes of the PII collection and connect the purposes to a USAID business function. Describe specifically how you will use the PII to accomplish the purposes provided in the previous section. Describe why the PII is necessary to accomplish the purposes. *Example:* The PII is collected on an application form and is used to determine eligibility for a new grant under the HIV/AIDs education program. *Example:* USAID is collecting the PII through an on-line survey to determine the effectiveness of USAID programs. The result of the survey will be analyzed by gender, age group, and ethnicity to determine outreach areas

for USAID's development programs.
AP-2 Purpose Specification

5.1.2 What are your procedures for identifying and evaluating any new uses of the PII?

In the case that PII is in the photo, video, or sound recording or in the captions, LPA will make a determination as to whether or not the individual will be named and their general location will be included (Hashtags of broad geographic locations, such as country). The determination to post PII will be made by the Deputy Assistant Administrator for Public Affairs and will be based on risk and privacy concerns.

If additional PII information becomes available or changes within the platform, LPA will contact the Privacy Office immediately to consult on the risks and privacy concerns associated with the change. After consulting with the Privacy Office, LPA will make a determination on the impact of the new PII.

If information may later be used for reasons other than the purposes specified in the public notices (PIA, SORN, and/or PA Notice), discuss how individual will be notified and discuss how any associated risks will be mitigated.

AP-2 Purpose Specification
AR-4 Privacy Monitoring and Auditing

5.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

The Accountability, Audit, and Risk Management Privacy Control Family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that USAID is complying with applicable privacy protection requirements and minimizing overall privacy risk.

5.2.1 Do you use any data collection forms or surveys?

(If you choose Yes*, please provide the OMB Control Number and USAID control number, and attach a copy of the forms and/or surveys in Appendix D to the PIA. Also, please attach a copy of or link to the Privacy Act Notice in Appendix D.)*

☒ No.

☐ Yes:

- ☐ Form
- ☐ Survey
- ☐ Other

Attach a copy of the form or the survey in Appendix D to the PIA. If there are multiple forms or surveys, attach a copy of the forms or surveys in the appendix and include a list in the response to this question within the PIA. State whether these forms or surveys include a Privacy Act Notice or Statement that describes the authorities to collect PII, the PII purposes and uses, and the effects on the individual of not providing the PII.

If you use data collection forms or survey, you must contact the USAID Information and Records Division

(M/MS/IRD) for assistance in ensuring that their forms comply with applicable statutes, regulations, policies, and procedures and for certifying their forms as part of the yearly USAID forms certification pursuant to ADS 505.
AR-2 Privacy Impact and Risk Assessment

5.2.2 If the PII is being moved from an old system to a new system, what safeguards are in place to reduce the privacy risks of moving the PII?
Not applicable.
Describe the procedures you have created to manage the risk of transferring PII from one system to another and how you will monitor those procedure to ensure that they work appropriately.
AR-2 Privacy Impact and Risk Assessment AR-4 Privacy Monitoring and Auditing

5.2.3 Who is involved in the development and/or continuing operation of the system and/or technology? *(Please check all that apply. Please provide the owners' and/or controllers' names for the items chosen.)*
☒ Mobile device manufacturer or other equipment manufacturer:
☒ Application Developer:
☒ Content Developer or Publisher:
☐ Wireless Carrier:
☐ Advertiser:
☐ Equipment or Device Vendor:
☐ Device User:
☐ Internet Service Provider:
☐ Third-Party Data Source (Data Broker):
☐ Other:
AR-3 Privacy Requirements for Contractors and Service Providers UL-1 Internal Use

5.2.4 Do you have a contract or other acquisition-related document for services involved with this system? What privacy requirements have you included in contracts and other acquisition-related documents, pursuant to the Federal Acquisition Regulation (FAR) and compliance with the Privacy Act, FISMA, and other privacy requirements?

(If you choose Yes, *please provide the Contract Number and attach a copy of or links to the contracts or other acquisition-related documents in Appendix D to this PIA.)*

☐ No.

☒ Yes:

The U.S. Government has negotiated terms of service with all of the social media outlets included in this assessment. The terms of service can be found at: http://www.howto.gov/social-media/terms-of-service-agreements/negotiated-terms-of-service-agreements

Provide the contract numbers and verification that the contract contains the appropriate privacy clauses pursuant to the FAR (48 CFR): 1) Part 24, Protection of Privacy and Freedom of Information; and 2) Part 52, Solicitation Provisions and Contract Clauses (52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act).

Please explain whether the privacy clauses cover third-party service providers and subcontractors to the contractors. You should include information on government contractors, cloud computing service provider contracts, and all other service-provider contracts and terms of service.

Describe the requirements you have included in contracts and other acquisition-related documents to ensure that 1) USAID owns and controls the PII in the system for the length of the contract and beyond, 2) the contractor or service provider has no ownership of the PII, and 3) the contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract during the life of the contract.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use

5.2.5 How do you audit and/or monitor system and user activity to ensure that the administrative, technical, and physical security safeguards you use actually do guard against privacy risks?

LPA undertakes semi-annual reviews of the systems to ensure that the Agency is guarding against privacy concerns. The Social Media Program Manager is responsible for these reviews.

Describe how you ensure that the PII is used in accordance with the stated practices in this PIA. Discuss auditing measures, as well as technical and policy safeguards such as information sharing protocols, special access restrictions, and other controls (for example, "read-only" access capability). Explain whether the system will conduct the audits or whether third parties, such as the Office of the Inspector General or the Government Accountability Office, will conduct reviews.

AR-4 Privacy Monitoring and Auditing

5.2.6 What training, awareness activities, and privacy rules of behavior do you use to ensure that USAID employees, contractors, and service providers understand their responsibility to protect PII and the procedures for protecting PII?

LPA will update its current standard protocol guide for those that have access to USAID social media accounts to include processes and procedures for managing the PII information that is available through the social platforms. The USAID social media protocol guide can be found here. In addition, LPA is ensuring that all of the Agency's Social Media account managers are taking the Account Management training that is in the LMS.

Describe privacy training and awareness activities, and provide any privacy rules of behavior documents.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
AR-5 Privacy Awareness and Training
UL-1 Internal Use

5.2.7 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?

(If you choose Yes*, please provide a copy of the forms or surveys as appendices to the PIA.)*

☒ No.

☐ Yes:

This question relates to the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 44 USC 3501 note, which provides restrictions on the use of statistical information when collected under a pledge of confidentiality.

If CIPSEA applies to your program, describe how you ensure that the PII is used for the specified statistical purposes only. Describe also how you ensure that the PII is not disclosed without the consent of the respondent. Describe how you ensure that, when the PII is disclosed without the respondent's consent, the disclosure is authorized by the USAID Administrator.

Statistical purpose (A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and (B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subparagraph (A).

Respondent means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

AR-2 Privacy Impact and Risk Assessment
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use
UL-2 Information Sharing with Third Parties

5.2.8 What other risks to privacy exist and how do you manage these risks?

Geotagging on Instagram and Flickr:

Geotagging is the process of including geographical information into or with any of a variety of media such as photographs, videos, blogs, websites and others. This process can happen automatically or manually and is the act of encoding geographical information such as latitude and longitude into common media, generally photographs and video. Web sites, blogs and the like don't encode the geographical information into the object but they can associate this information with a post or blog, for example.

Geotagging can pose significant privacy or even life threatening risks. Can allow others to identify the location where a picture was taken (e.g., using free browser plug-ins), to track an individual's location, or to correlate such data with other information. The use of locational data to report an individual's movements, whereabouts or actions online in real time (e.g., on social networking sites or other public platforms, to track where an individual may be shopping, eating, sleeping, etc.) can enable "cyberstalking" or "cybercasing" (i.e., use of such information to commit real-world crimes).

Geotagging can reveal details specific details such as location and identification of people and places; collateral (non-subject of a post or photograph) location of people and places, location of children or other family members at school, hangouts, home, and work; and location of personal property. Moreover, geotagging can reveal the daily commute, shopping habits, and office and home addresses of individuals, as well as such information about their family members, friends, and business associates. Geotagging enables tracking of individuals and assets by criminals, foreign intelligence services, and terrorists.

In addition, some web sites now will search themselves and other sites to see if any individuals were tagged by name and through facial recognition functions and then will automatically tag the individuals it recognized in a photograph. In conjunction with geotagging, name and facial recognition tagging can produce an image that has the names of individuals in photos along with their location at a specific time and date. This is a relatively new technology, but it is rapidly becoming more common.

Because photos may be uploaded directly to Instagram and then shared through Instagram's mobile applications or the integrated social media sites, the use of Instagram may present location-based privacy concerns when uploaded photos can be used to identify a user's location at a given point in time. Location-based privacy issues are a particular issue for users who select the option to automatically create a posting in Foursquare when an Instagram photo is uploaded. Location-based privacy concerns are endemic to many mobile applications, and users must exercise discretion with mobile applications.

The best option for managing the privacy risks of geotagging is to not use it; that is, to disable the functions on all devices, including smart phones, tablets, and cameras, and in all social media platforms, including Instagram, Facebook, Twitter, Gowalla, Foursquare, and Flickr. However, it is not always possible to discover all of the settings and ways that systems use geotagging and GPS tools. Therefore, when using social media, there is always a certain amount of privacy risk.

RISK MITIGATION: The Agency has decided not to implement geotagging at this time. The Agency will make a risk and privacy determination on if and when geo-tagging will be enabled. In this circumstance the Deputy Assistant Administrator for Public Affairs in LPA will make the determination, after working with the Privacy Office to update the PIA, pursuant to ADS 508 Privacy Program Section 3.5.2, Privacy Impact Assessments.

Mobile Hardware Devices:

Individuals who use their mobile and non-mobile devices and equipment to create digital content (e.g., word processing documents, photos) may be unaware of the extent or nature of metadata that is automatically generated with such content, and may not be able (or know how) to prevent the creation of such metadata or its transmission to or collection by others with their digital content. For example, digital photos may be encoded in Exchangeable Image File Format (EXIF) with time, date, location or other photo-related data that can be traced to the individual. No centralized technical measure can be implemented, because Instagram is a mobile application.

Also, Mobile hardware devices can capture and record audio, video, or other data, including the generation of metadata about the user (e.g., digital photos may also contain metadata such as name, location, device ID, etc.). Could be hijacked, turned on or off, and otherwise controlled remotely to spy on the user or others.

RISK MITIGATION: LPA will work with the CIO to develop a standard mobile device configuration to change the default settings for all Agency Instagram users and train all Instagram users to implement the standard mobile device configuration to disable features not wanted, such as geotagging.

Mobile Applications:

Mobile applications (apps) are Software pre-installed or downloaded on demand to a mobile device in order to enable or facilitate specific types of transactions or data access (e.g., mobile payments, social networking, access to Government services or accounts). Some apps may contain malware that may compromise the host device, including any PII that the device stores or transmits. Apps may not fully or properly disclose what PII they are accessing from the device, or may access more PII than needed. App security may not be fully vetted by the platform provider.

Mobile device manufacturers or other original equipment manufacturers (OEMs) may make design decisions to manage user experience that create privacy vulnerabilities. For example, in order to make photo apps more efficient, an OEM may permit apps that request location data to have access to other device data (e.g., photos, address books), even if the app functionality does not require such access. Developers and platforms of Instagram and applications used with Instagram may exploit vulnerabilities created by OEMs. For example, app developers may design applications that exfiltrate photos once the device user permits the app's access to location data.

LPA uses the mobile applications for Facebook, Instagram, and Twitter, but not for the other social media platforms.

RISK MITIGATION*:* LPA will work with the CIO to develop a standard mobile device configuration to change the default settings for all users of Instagram and related applications. And LPA will train all Facebook, Instagram, and Twitter users to implement the standard mobile device configuration to disable features not wanted, such as geotagging.

Storify and Facebook connection:

Users can post private updates from Facebook publicly on Storify. By using their curation tool, someone in a private or secret Facebook group (where only members can view content) can share something meant for a limited audience for the whole web to view on Storify.

RISK MITIGATION: Because USAID does not "friend" people on Facebook (people "like" USAID), content that is posted as private on Facebook would never be available to USAID. The Storify privacy risk is more focused on an individual that would have access to a user's private information, which USAID does not do through its corporate accounts.

5.3 DATA QUALITY AND INTEGRITY (DI)

The Data Quality and Integrity Privacy Control Family enhances public confidence that any PII collected and maintained by USAID is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

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

The social media platforms collect PII directly from users. USAID will not collect, use, maintain, or disseminate the PII that the social media platforms collect from their users.

The nature of the LPA use of the social media platforms will require LPA to collect any PII directly from the individuals who are in the photos, videos, or sound recordings that USAID will post. Therefore, USAID will ask for permission via e-mail, in person, or through the social medial platforms prior to posting any PII.

Discuss whether the PII is collected directly from the individual or collected from another source. If the PII is not being collected from the individual, but from sources other than the individual, you must explain why collecting the PII from other sources is required. Sources other than the individual may include other individuals, systems,

systems of records, businesses, commercial data aggregators, other Federal agencies, and state or local agencies.

Describe your sources of information when you use digital collaboration tools or services and/or mobile services.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

DI-1 Data Quality

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

Prior to posting information on the social media platforms, LPA will do a quality assurance review of all information included in the post. LPA's Social Media Program Manager will also ensure that information is complete.

Describe how what reasonable steps you take to confirm the accuracy and relevance of PII. Such steps may include editing and validating addresses as they are collected or entered into the system using automated address verification look-up application programming interfaces. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

DI-1 Data Quality

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

LPA's Social Media Program Manager will review the PII posted on the social media platforms on a semi-annual basis to ensure that the PII is correct.

Describe how you will ensure that the PII continues to remain accurate, relevant, timely and complete over time. Describe what reasonable steps you take to confirm the accuracy and relevance of PII after the initial collection of the PII. Such steps may include periodic quality control auditing.

DI-1 Data Quality

5.4 DATA MINIMIZATION AND RETENTION (DM)

The Data Minimization and Retention Privacy Control Family helps USAID to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. USAID retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

5.4.1 What is the minimum PII relevant and necessary to accomplish the legal purpose of the program? *(Please explain the business need for the PII.)*
Images that in some circumstances include individuals should be considered a minimum PII element. In addition to this, names of individuals and general locations (not specifically geo-tagging) such as Kenya would typically be included in this. See PIA Section 5.2.1 for specifics.
Describe why you need the specific PII elements that you collect in order to fulfill the business functions of the program. If you use SSNs, please explain why you need SSNs to fulfill a business function and why your program could not operate without them. Example: You might collect name and email address in order to contact members of the public who comment on USAID programs on your web site, but do not collect addresses and phone numbers, because email addresses are sufficient to contact such people. Describe any impacts on business functions from not being able to collect, use, maintain, or disseminate the specific PII elements. Describe any decision made to collect less data than originally planned. Align your explanation with the Purpose section of any relevant System of Records Notice (SORN). A general statement about the purpose without discussing particular PII is not an adequate response.
DM-1 Minimization of Personally Identifiable Information

5.4.2 How do you monitor the PII and the system to ensure that only the PII identified in the privacy notices is collected, used, maintained, and disseminated by the system and that the PII continues to be necessary to accomplish the legally authorized purpose?
LPA's Social Media Program Manager will undertake a semi-annual review of the PII posted on the applications to ensure that all PII is legally authorized.
Describe how you ensure that you do not collect more PII than stated in the privacy notice. Describe how you ensure that all of the PII elements collected continue to be necessary for the stated purpose.
AR-4 Privacy Monitoring and Auditing DM-1 Minimization of Personally Identifiable Information

5.4.3 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?

(If you choose Yes*, please explain.)*

☒ No. Storify aggregates information from different social media platforms. However, because of the nature of the accounts that USAID has set-up, we would not be able to access, view, or pull information that is posted privately on any users pages.

☐ Yes:

Discuss whether the system will aggregate or derive data. State whether a unique identifier may be generated by the system and provided to the user for future follow up. Describe how the new PII will be used and why it is relevant and necessary to the system.

Modernized systems often have the capability to derive new data and create previously unavailable data about an individual through aggregation of the information collected. The *mosaic effect* is the idea that disparate pieces of information, though individually of limited or no value, can be significant when combined with other pieces of information that could result in an unforeseen vulnerability, exploitation or misuse of the information.

Derived data is information obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information.

Data aggregation is the taking of various data elements and then turning them into a composite of all the data to form another type of data (i.e., tables or data arrays) that is usually different from the source information.

DM-1 Minimization of Personally Identifiable Information

5.4.4 What types of reports about individuals to do produce from the system?

LPA creates general reports to track the number of users who "follow", "friend", or "like" USAID postings. These reports do not pull PII and are used for measuring the effectiveness of the social media tool. See PIA Section 5.9.1.

Describe each report that will be produced and what PII will be included. Discuss the use for the reports, and who will have access to the reports inside and with whom you will share the reports outside USAID.

In addition, discuss whether the report will produce anonymized data. If data will not be anonymized, discuss why. Explain the risks that the PII can be combined with other data either to identify an individual or used in ways that the individual did not intend.

Anonymized data means data from which the individual cannot be identified by the recipient of the information. Sometimes known as de-identified. To anonymize or de-identify PII in a report, individuals' names, addresses, and full postal/zip codes must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the individual.

DM-1 Minimization of Personally Identifiable Information

5.4.5 How do you file, maintain, and store the PII? How long do you retain the PII? What methods do you use to archive and/or dispose of the PII? How do you ensure that the records management retention rules specified above are followed?

Any PII posted on social media will be maintained in that social media platform. LPA will store and destroy electronic PII in accordance with methods described in ADS 545mak, Data Remanence Procedures, and ADS 545mas, Media Handling Procedures and Guidelines. In addition, LPA will retain and dispose of PII in accordance with the National Archives Records Administration's General Records Disposition Schedules and the agency's approved disposition schedules.

The program manager, in consultation with a records management officer in the USAID Information and Records Division (M/MS/IRD), must develop a records retention schedule for the records contained in the system. After the records schedule is developed, it is sent to the National Archives and Records Administration (NARA) for approval. Consult with your records management office for assistance with this question.

If a NARA-approved records schedule exists, please provide the records schedule and explain for how long and for what reason the PII is retained. If a general records schedule (GRS) covers the information, then please provide the GRS number (GRS X, Item X) and explain for how long and for what reason the PII is retained.

If there is not an approved NARA records schedule or GRS, then the project manager should consult with the records management officer to develop a records retention schedule for the records contained in the system for the minimum amount of time necessary to fulfill the needs of the project. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

Describe the processes used to dispose of the PII when it is no longer needed.

Describe how you ensure that the PII is retained only as long as it is needed and that the PII is destroyed in an appropriate manner.

AR-4 Privacy Monitoring and Auditing
DM-2 Data Retention and Disposal

5.4.6 Does the system monitor or track individuals?

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

☒ No.

☐ Yes:

Describe how you monitor individuals, and explain the purpose of the monitoring. Discuss whether someone reviews any logs created by the monitoring. Discuss the safeguards you have created to prevent abuse. Include how the decision was made to move forward with a monitoring capability and what safeguards are in place to reduce impact on personal privacy. If the system has the capability to monitor individuals, but that capability is not be used, describe how you will ensure that such monitoring capability will not be used.

Describe how you track individuals by using tracking technologies that will compile or make such data available to USAID. Describe how other persons or agencies (app developer, original equipment manufacturer, network or carrier, cloud service provider) will use tracking technology. Describe how the system could enable other persons or agencies to determine the location of individuals and whether such location data could compromise the physical safety of the individuals or the security of USAID operations.

IP-1 Consent
TR-1 Privacy Notice

5.4.7 What policies, procedures, and control methods do you follow to minimize the use of PII for and protect PII during testing, training, and research?
LPA has a social media policy that ensures the minimum use of PII. The social media policy can be found here. In addition, the Social Media Program Manager of the social media accounts will ensure that these policies and procedures are being followed.
Discuss whether you use PII for testing update or new applications prior to deployment and whether you also use PII for research purposes and for training. The use of PII in testing, research, and training increases the risk of unauthorized disclosure or misuse of the PII. Describe the measures you take to minimize any associated privacy risks. Also provide the authorities that allow you to use PII for testing, training, and research.
AP-2 Purpose Specification AR-4 Privacy Monitoring and Auditing DM-3 Minimization of PII Used in Testing, Training, and Research

5.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

The Individual Participation and Redress Privacy Control Family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in USAID decisions made based on the PII.

5.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?
Prior to posting PII, LPA will request consent from individuals to post their PII. This will be either through e-mail, in person or through the social media application.
Discuss whether the PII collection is mandatory or voluntary and how the information is collected, such as via an application form, survey, web form, or extracted from other systems. Discuss whether an individual has the opportunity to consent to specific uses or whether consent is given to cover all current uses of the PII. Describe the process by which consent is given. If the individual can decline or opt out, describe how this is done. Describe the process by which consent is obtained for new uses of the PII after the initial collection. If no opportunities are available to individuals to consent, decline, or opt out, please explain why not.
IP-1 Consent TR-1 Transparency

5.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?
LPA will provide in its profiles the LPA contact information for an individual wishing to amend the PII that USAID has posted. LPA can remove or amend content from social media content posted and controlled by USAID.
Describe any procedures you provide for individuals to access their PII and to request correction or amendment of their PII, ***in addition to*** the USAID Freedom of Information Act (FOIA) and/or Privacy Act procedures under 22 CFR Part 215. If you provide such additional access and amendment procedures, describe how you, consistent with the Privacy

Act, keep (for the life of the record or five years after disclosure) an accurate accounting of disclosures of PII including 1) date, nature, and purpose of each disclosure; and 2) name an address of the person or federal agency to which the disclosure was made.

If individuals cannot access or amend or correct their PII under the USAID FOIA/Privacy Act procedures, explain why not.

Person means any individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision.

AR-8 Accounting of Disclosures
IP-2 Individual Access
IP-3 Redress

5.5.3 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?

LPA will provide in its profile the LPA contact information for an individual wishing to amend the PII that USAID has posted. LPA can remove or amend content from social media content posted and controlled by USAID, but cannot provide a mechanism to provide access to or amendment of content that it posted but which has been reused by other social media users.

A social media user may request the platform to amend content, but the platforms retain the right to remove, edit, block, and/or monitor content that it determines in its sole discretion violates the terms of use.

Describe how you ensure that the program manager is able to produce the records when an individual requests access to and amendment of his/her personal information through the USAID Freedom of Information Act or Privacy Act request process. Please explain whether your protections cover records or systems controlled by third-party service providers and/or subcontractors to contractors.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
IP-2 Individual Access
IP-3 Redress

5.6 SECURITY (SE)

The Security Privacy Control Family supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by USAID against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

5.6.1 How do you secure the PII?

USAID will not collect, use, maintain, or disseminate PII from the individuals who use the social media platforms or visit USAID accounts.

LPA will post on social media platforms PII such as name, image, and temporary location (Hashtags of broad geographic locations of photos, such as country). Locations will only be used during special circumstances, which were outlined in the section above. If PII information outside of this scope gets posted on social media platforms, the Social Media Program Manager will ensure that such PII is removed promptly. See PIA Section 5.4.2 for specifics related to monitoring the PII posted.

In the case that photos, videos, sound recordings, captions, or hashtags with PII is posted, LPA will make a determination as to whether or not the person will be named and their general location will be included (Hashtags of broad geographic locations of photos, such as country). Geotagging will not be used at this time. The determination to post PII will be made by the Deputy Assistant Administrator for Public Affairs and will be based on risk and privacy concerns.

Describe the administrative, technical, and physical security safeguards you use to guard against privacy risks such as 1) data loss or breach; 2) unauthorized access, use, destruction, or modification; 3) unintended or inappropriate disclosure; or 4) receipt by an unauthorized recipient.

Provide an overview of the mitigation strategies you use to protect the PII collected, used, maintained, and disseminated by your system.

Describe the steps taken to ensure that the PII is used appropriately. Indicate any physical controls that will be implemented (security guards, identification badges, key cards, safes, locks, etc.). Indicate any technical controls that will be implemented (user identification, password, intrusion detection, encryption firewall, etc.). List any administrative controls that will be implemented (periodic security audits, regular monitoring of users, backup of sensitive data, etc.). Describe any mechanisms in place to identify security breaches. Discuss what privacy incident reporting plan and procedures are in place to effectively handle a privacy incident involving the system.

Describe the extra mitigation strategies do you use to guard against the heightened privacy risks associated with any collection, use, maintenance, or dissemination of Names with SSNs.

Example: Describe the steps you take to make sure that transmitted data is properly secured through encryption or by classified couriers.

Example: Describe the steps you take to develop or modify processes and procedures to account for identified privacy risks related to the increased frequency of access to audit logs.

SE-1 Inventory of Personally Identifiable Information
SE-2 Privacy Incident Response

5.6.2 If your system is controlled by a contractor or service provider, what requirements have you included in contracts and other acquisition-related documents about the procedures for privacy breach liability and response?
The Terms of Use and "Amended Terms for Federal, State, and Local Governments of the United States" control USAID activities on the social media platforms. These terms of service have been negotiated by GSA and are posted on http://www.howto.gov/social-media/terms-of-service-agreements/negotiated-terms-of-service-agreements
Describe how you ensure that government contractors and cloud computing service providers have privacy incident response procedures and that they follow those procedures. Explain whether the contract language allocates any responsibility and liability for privacy breach response.
AR-3 Privacy Requirements for Contractors and Service Providers AR-4 Privacy Monitoring and Auditing SE-2 Privacy Incident Response

5.7 TRANSPARENCY (TR)

The Transparency Privacy Control Family ensures that USAID provides public notice of its information practices and the privacy impact of its programs and activities.

5.7.1 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; and 4) The effects on the individual, if any, of not providing all or any part of the PII?
LPA will provide on all social media accounts an information link to the Agency's Privacy Policy website, which can be found at: http://www.usaid.gov/privacy-policy. Prior to posting PII, LPA will get consent from individuals directly for the use of their PII. USAID has also published a System of Records Notice entitled USAID-29 On-Line Collaboration Records, which provides notice to individuals on these issues.
Provide a copy of any written notice that you provide before you collect, use, maintain, or disseminate PII, including any: 1) posted privacy policy; 2) Privacy Act Statement, pursuant to the Privacy Act (e)(3); on forms or surveys; 3) System of Records Notice; or 4) other information provided on the USAID web site. Provide a copy of any notice you provide directly to the individuals whose PII you collect. If you collect the PII from someone other than the individual, explain how that PII is collected and how the individual is provided notice. If notice was not provided, explain why not. Describe how you monitor or audit privacy notices to ensure that on a continuing basis the notice statements are accurate and appropriately placed.
AR-4 Privacy Monitoring and Auditing TR-1 Privacy Notice TR-2 System of Records Notices and Privacy Act Statements

5.7.2 Have you or will you publish a Privacy Act System of Records Notice (SORN) for this system?
(If you choose Yes*, please provide information about the SORN, including the name, date, and Federal Register citation.)*
☐ No
☒ Yes: USAID-29 On-Line Collaboration Records, 75 FR 4526 (Jan. 28, 2010).
For all systems of records, the Privacy Act requires that the agency publish a SORN in the Federal Register. See **ADS 508 Privacy Program** Section 508.3.10.2 and **SORN Template**. Include the Federal Register citation for the SORN. If the information used in the project did not require a SORN, explain why not. In some instances, an existing SORN (either program-specific, USAID-wide, or Government-wide) may apply to the system's collection of information. In other instances, a new SORN may be required. USAID SORNs are available at http://www.usaid.gov/privacy-policy/systems-records-notices-sorns. That web page also has links to government-wide SORNs, which might be applicable to your system of records. If a government-wide SORN covers your records, you do not need a USAID-specific SORN.
TR-2 System of Records Notices and Privacy Act Statements

5.7.3 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?
U.S. Government has amended terms of service with all of the social media outlets included in this document. They are found at: http://www.howto.gov/social-media/terms-of-service-agreements/negotiated-terms-of-service-agreements
Describe how you ensure that any cloud computing services providers do not move the PII without notice to you.
AR-3 Privacy Requirements for Contractors and Service Providers AR-4 Privacy Monitoring and Auditing TR-2 System of Records Notices and Privacy Act Statements

5.8 USE LIMITATION (UL)

The Use Limitation Privacy Control Family ensures that USAID only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

5.8.1 Who has access to the PII at USAID?

LPA will not collect, use, maintain, or disseminate the PII of social media users through its use of any of the social media accounts. These social media sites are public platforms or accessible for free upon registration, any individual with access to the internet will have access to the PII posted on these social media accounts. However, only authorized staff members will have the authority to post PII via access to the USAID social media accounts.

Identify who within USAID, its contractors, and its service providers will have access to the PII. Describe what USAID offices and what types of USAID employees, contractors, and service providers have access to the PII. Also, include the level of access for each office and type of worker; that is, what PII to which they have access, the purpose of the access, and how they get access to the PII. Describe the procedures you use to determine which users may access the information and how you determine who has access.

UL-1 Internal Use

5.8.2 How do you monitor access to and use of the system to ensure that the PII is collected, accessed, and used only 1) for the authorized purposes and 2) by authorized USAID employees, contractors, and service providers?

LPA's Social Media Program Manager will be responsible for monitoring access to and the use of the social media platforms. LPA will update the Agency's social media guidelines to cover specific information about use of all of the nine social media platforms included in this PIA. LPA will provide the updated social media guidelines to the Privacy Office at privacy@usaid.gov.

Describe how you ensure that the system uses PII only in ways that are compatible with the specified purposes.

Describe what USAID offices and what types of USAID employees, contractors, and service providers have access to the PII. Also, include the level of access for each office and type of worker; that is, what PII to which they have access, the purpose of the access, and how they get access to the PII. Describe the procedures you use to determine which users may access the information and how you determine who has access.

AR-3 Privacy Requirements for Contractors and Service Providers
AR-4 Privacy Monitoring and Auditing
UL-1 Internal Use

5.8.3 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?

These social media accounts are public platforms or accessible for free upon registration, information posted on these social media accounts is available to anyone that has access to the Internet or mobile applications.

Discuss the sharing of PII outside USAID. Identify the name of each system, person, or federal agency outside of USAID with whom you share PII, what PII you share, the purpose of the sharing, and how you share the PII (such as on a case-by-case basis, US mail, bulk transfer, or direct access).

Explain any use of the system or related web site or application that would make data assets available to the public, including 1) what data assets will be posted; 2) how the public will be able to interact with USAID; and 3) how the public will be able retrieve or use the data assets.

Person means any individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political

subdivision of a State, territory, tribal, or local government or a branch of a political subdivision.
UL-2 Information Sharing with Third Parties

5.8.4 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?

(If you choose Yes, please provide the specifics of the agreement or a copy of the agreement.)

☐ No.

☒ Yes: These social media accounts are public platforms or accessible for free upon registration, information posted on these social media accounts is available to anyone that has access to the Internet or mobile applications.

In the case that PII is in the photo, video, or sound recording or in the captions, LPA will make a determination as to whether or not the individual will be named and their general location will be included (Hashtags of broad geographic locations, such as country). The determination to post PII will be made by the Deputy Assistant Administrator for Public Affairs and will be based on risk and privacy concerns.

If additional PII information becomes available or changes within the platform, LPA will contact the Privacy Office immediately to consult on the risks and privacy concerns associated with the change. After consulting with the Privacy Office, LPA will make a determination on the impact of the new PII.

State whether there is a MOU, contract, or agreement in place and define the parameters of the sharing agreement. Describe any agreement that covers the terms of the information sharing, including 1) a specific description of the PII covered, 2) an enumeration of the purposes for which the PII may be used, 3) monitoring, auditing, and training requirements, and 4) the consequences for unauthorized access to and use of the PII.

Describe what privacy controls you use to reduce the risk of transmitting data to systems outside of USAID. Describe how the data is transmitted outside of USAID. For example, describe whether the data transmitted electronically, in bulk, by paper, direct access, or by some other means. Discuss whether access controls have been implemented to ensure appropriate sharing of information.

Discuss whether the receiving system has undergone a Certification & Accreditation (C&A). For sharing with non-Federal agencies, discuss how the relevant privacy protections have been expressed and documented to ensure the privacy and security of the information once it is shared. If necessary, discuss the provisions for notification of a privacy incident and who owns the liability for such incident.

When using digital collaboration services and/or mobile services, describe how you will share data outside of USAID. Specifically, describe how you will expose or transmit the data to a third-party or how the third-party will access the data.

Digital refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency.

Mobile denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms.

AR-4 Privacy Monitoring and Auditing
UL-2 Information Sharing with Third Parties

5.9 THIRD-PARTY WEB SITES AND APPLICATIONS

The OMB policy in *Guidance for Agency Use of Third-Party Web sites and* Applications, M-10-23 (June 25, 2010), requires USAID to take specific steps to protect individual privacy whenever it uses third-party web sites and applications to engage with the public. Through the following questions, USAID ensures individual notice and careful analysis of the privacy implications when using third-party web sites and/or applications. Please answer the following questions, if your system involves a third-party web site or application.

The term "*third-party web sites or applications"* refers to web-based technologies that are not exclusively operated or controlled by a government entity. Often these technologies are located on a ".com" web site or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official web site.

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

Facebook: Users do not have to subscribe to Facebook in order to view our Facebook page. In order to "like" or comment on the USAID page, users may choose to set up an account with Facebook. Information provided in the account set up process is owned and managed by Facebook and subject to Facebook's privacy policy. USAID will not seek out or collect account information held by Facebook. Some Facebook users choose to reveal their actual name, photo, or other personal information in their profile or comments. Some Facebook users may also append their location to their posts.

Flickr: Users do not have to sign-up for Flickr to view USAID's photos. However to comment, star, or subscribe to USAID's page, users would need to create a Flickr account. The only PII that could be available through Flickr would be that which a user posts on their personal Flickr page and therefore not under the control of USAID.

GitHub: This is an external website, managed and hosted by a private company with no relationship to USAID. USAID will post content on this page, but all content will have been previously made public. No sensitive information will be posted. GitHub requires users to register before posting a software project or viewing or editing software code posted by other users. To register, users must provide a username and email address. Users can create an expanded profile that includes a name, username, website URL, company name, location, professional biography, and a profile picture or avatar. USAID will not collect PII through its use of GitHub. USAID will be able to view the profiles of other GitHub users, including users who edit USAID software code posted on GitHub. If a GitHub user interacts with USAID through its official GitHub webpage, their name, username, email address, website URL, company name, location, professional biography, profile picture or avatar, or any other PII provided by the user might be made available to USAID.

Instagram: There are millions of Instagram users world-wide, including all types of people, government agencies, and private organizations. Instagram requires users to create an account before using the web site. To create an account, users must provide their username, password, and email address. Users may choose to provide a profile with additional information such as full name, photo, phone number, gender, location, descriptions of users' skills, professional experience, educational background, honors, awards, professional affiliations, LinkedIn Group memberships, networking objectives, and companies or individuals that users follow. Users may choose to provide such information in order to be "found" and therefore connect with other users. If an Instagram user interacts with USAID through its official Instagram account (including commenting on a USAID photo), requests information, or submits feedback through Instagram, their Instagram username will become available to USAID. Other PII provided by the user, including first and last name, profile photo, images, and contents of postings, may also become available to USAID. However, USAID does not collect, use, maintain, or disseminate PII through its use of Instagram. USAID will only track the number of users who "follow" or "like" USAID photos. If users "follow" or "like" a USAID photo, the fact that the user made that selection will be publicly available. USAID does not record which users "follow" or "like" its photos. Whenever possible, USAID elects not to have non-public information

made available to it. To our knowledge, Instagram does not make non-public information available to USAID based upon a user's "following" or "liking" USAID photos. USAID will not "follow" or "like" other photos posted by other users. USAID will only note the number of actions taken in regard to USAID photos. This will be a mobile application that is available on phones, however only LPA staff will have access to the USAID Instagram account.

LinkedIn: This is an external website, managed and hosted by a private company with no relationship to USAID. USAID will post content on this page, but all content will have been previously made public. No sensitive information will be posted. LinkedIn requires users to create an account before using the website. To create an account, users must provide their name, email address, and password. Users can provide additional information such as gender and location. In addition, users may choose to provide a profile with additional information such as photos, descriptions of users' skills, professional experience, educational background, honors, awards, professional affiliations, LinkedIn Group memberships, networking objectives, and companies or individuals that users follow. USAID will not collect PII through its use of LinkedIn. USAID will be able to view the profiles of LinkedIn users, including users who chose to join the USAID group. If a LinkedIn user interacts with USAID through its official LinkedIn webpage, their name, photo, and professional and educational history, or any other PII provided by the user might be made available to USAID.

Storify: Users can post private updates from Facebook publicly on Storify. By using their curation tool, someone in a private or secret Facebook group (where only members can view content) can share something meant for a limited audience for the whole web to view on Storify.

Tumblr: Users can view USAID's Tumblr page without having a Tumblr account. However to follow, like or repost anything from USAID the user would need to have their own account. It is possible for USAID to repost a Tumblr users post, that could potentially include PII. If USAID wants to repost something from Tumblr that includes PII, we will seek permission from the user before reposting this information.

Twitter: Users do not have to subscribe to Twitter in order to view our Twitter feed. In order to "follow" USAID, users may choose to set up an account with Twitter. Information provided in the account set up process is owned and managed by Twitter and subject to Twitters privacy policy. USAID will not seek out or collect account information held by Twitter. Some Twitter users choose to reveal their actual name, photo, or other personal information in their profile or Tweets. Some Twitter users may also append their location to their Tweets. USAID does not intend to collect, maintain, or disseminate personally identifiable information (PII) from the individuals who visit or follow our Twitter account. We will, however, occasionally gather publicly available information on Twitter for internal reporting purposes. This may include Tweets that mention USAID or users who ReTweet our posts. The Twitter handles of organizations, journalists, and influential bloggers may be collected and distributed for use in the daily news clips. For instance "@gatesfoundation and 7 others re-Tweeted our post leading to 750,000 additional views" These will be maintained in the same manner as press clips. Other than the press clips mentioned above, USAID will not be collecting, sharing, storing, or maintaining any PII.

YouTube: Users do not have to subscribe to YouTube in order to view our YouTube channel. In order to comment on the USAID channel, some users may choose to set up an account with YouTube. Information provided in the account set up process is owned and managed by YouTube and subject to YouTube's privacy policy. USAID will not seek out or collect account information held by YouTube. Some YouTube users choose to reveal their actual name, photo, or other personal information in their profile or comments. USAID does not intend to collect, maintain, or disseminate personally identifiable information (PII) from the individuals who visit or comment on our YouTube channel.

Describe the specific types of PII and data your technology makes available to USAID. Also, describe separately the specific types of PII and data your technology makes available to contractors and service providers. Please refer to Question 4.2.1 for specific types of PII and Question 4.2.3 for specific types of digital and mobile related data.

Make PII available includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the web site or application. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Describe how you will handle any PII that becomes available to you beyond what you are authorized and have a

business need to collect, use, maintain, or disseminate.
AP-1 Authority to Collect

5.9.2 How do you ensure that the privacy policy of the third-party web site and/or application is reviewed to ensure that it appropriately supports the USAID privacy protection position?

(Please attach a link to or a copy of the privacy policy in Appendix D to this PIA.)

USAID has reviewed the privacy policies of each of the social media web sites. The USAID web site privacy policy can be found at http://www.usaid.gov/privacy-policy. Each page or account will have a link back to the USID web site privacy policy on usaid.gov. The privacy policies for each of the social media web sites can be found at:

Facebook: https://www.facebook.com/about/privacy/

Flickr: https://info.yahoo.com/privacy/us/yahoo/flickr/details.html

GitHub: https://help.github.com/articles/github-privacy-policy

Instagram: http://instagram.com/about/legal/privacy/

Storify: https://storify.com/privacy

Tumblr: http://www.tumblr.com/policy/en/privacy

Twitter: http://twitter.com/privacy

YouTube: http://www.youtube.com/t/privacy

Explain how you ensure, in consultation with legal counsel and relevant program managers, that the content of the third-party public notices comply with USAID privacy requirements. Please provide a link to the privacy policy.
AR-3 Privacy Requirements for Contractors and Service Providers TR-1 Privacy Notice

5.9.3 If you have a link from USAID.gov to this third-party web site or other location that is not a part of an official government domain, do you provide an alert (such as a statement or "pop-up") to visitors explaining that they are being directed to a non-governmental web site that may not afford the same privacy protections as USAID?

Yes, USAID includes the standard disclosure language that the user is departing USAID.gov for a third-party web site for each of the social media sites.

Describe how you explain to the public that the web site or application is not a government web site or application, that it is controlled or operated by a third party, and that the USAID Web site Privacy Policy does not apply to this third-party web site or application.
AR-3 Privacy Requirements for Contractors and Service Providers TR-1 Privacy Notice

5.9.4 If you incorporate or embed the third-party application on the USAID web site, how do you disclose to the public their use of the third-party application?
(If you choose Yes*, please describe the disclosure.)*
Not applicable.
A copy of the USAID Web site Privacy Notice is provided at http://www.usaid.gov/privacy.html. If the collection and/or storage of PII through your third-party application is different from the process described in the USAID Web site Privacy Notice, please describe the third-party application involvement. For example, the third-party web site can provide individuals with itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, the third-party web site must include consent mechanisms to ensure that the web site operations comply with individual choices.
TR-1 Privacy Notice

5.9.5 How do you create the appropriate USAID brand to indicate an official USAID presence on the third-party web site, and how you distinguish USAID activities from those of non-governmental actors?
Each USAID page or account will be marked by the USAID brand on the top left corner of the page or account. In addition, any USAID profile will include a link to http://www.usaid.gov/privacy-policy. And the page or account will also provide the USAID mission statement when space is available.
Describe how you apply appropriate branding to distinguish USAID activities from those of non-governmental actors, when you use a third-party web site or application that is not part of an official government domain. For example, do you, to the extent practicable, add the USAID seal or emblem to the USAID profile page on a social media web site to indicate that it is an official agency presence? Please list activities that a government individual can perform on this third-party web site or application that the public is not allowed to see.
TR-1 Privacy Notice

Please stop here and send this form to the Privacy Office at privacy@usaid.gov. The Privacy Office will review your information and contact you.

- If more information is needed, the Privacy Office will contact you with questions or will send you the appropriate form(s) to complete.
- If this PIA is ready for the approval process, the Privacy Office will send you this form to sign.

6. APPENDICES

6.1 APPENDIX A GLOSSARY

The following table describes terms and abbreviations used in this document.

Table 5-1 Glossary

Abbreviations	Description
ADS	USAID Automated Directives System
Alien	Someone who is not citizen of the United States or an alien lawfully admitted for permanent residence.
Anonymized Data	Data from which the individual cannot be identified by the recipient of the information. The name, address, and full post code must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the individual.
Automated Directives System	
C&A	Certification & Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (Software as a Service, Platform as a Service, Infrastructure as a Service), and four deployment models (private cloud, community cloud, public cloud, hybrid cloud). (NIST SP 800-145)
CISO	Chief Information Security Officer
D	Draft Version
Data Aggregation	The taking of various data elements and then turning them into a composite of all the data to form another type of data (i.e., tables or data arrays) that is usually different from the source information
Derived Data	Information obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information
Digital	Refers generally to data in electronic or other non-paper format, such as internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency
F	Final Version
FIPS PUB	NIST Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
Foreign Service National Direct Hire (FSNDH) Employee	Means 1) a non-U.S. citizen employee hired by a USAID Mission abroad, whether full or part-time, intermittent or temporary, and inclusive of a Third Country National (TCN) who is paid under the local compensation plan (LCP), and 2) who was appointed under the authority of the Foreign Service Act of 1980.
Foreign Service National Personal Services Contractor (FSNPSC) Employee	Means 1) a non-U.S. citizen employee hired by a USAID Mission abroad, whether full or part-time, intermittent, or temporary, and inclusive of a Third Country National (TCN) who is paid under the local compensation plan (LCP), and 2) who entered in a contract pursuant to the AIDAR, Appendix J.
IA	Information Assurance, Office of the Chief Information Security Officer
IIF	Information in Identifiable Form

Individual	A citizen of the United States or an alien lawfully admitted for permanent residence. (5 USC 552a)
Information in Identifiable Form (IIF) *See Personally Identifiable Information*	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (for example, name, SSN, date of birth, or medical history (44 USC 3501, note § 208); or information permitting the physical or online contacting of a specific individual. (M-03-22)
Information System Security Officer (ISSO)	Individual responsible to the senior agency information security officer, AO, or information SO for ensuring the appropriate operational security posture is maintained for an information system or program. (Chapters 508 and 545)
Information Technology	Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use— (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related re- sources; but does not include any equipment acquired by a federal contractor incidental to a federal contract (40 USC 11101); or any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (M-03-22)
M	Memorandum or Bureau of Management
Make PII Available	Includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the web site or application. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.
Mobile	Denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms
Mosaic Effect	When disparate pieces of information, though individually of limited or no value, can be significant when combined with other pieces of information that could result in an unforeseen vulnerability, exploitation or misuse of the information
MOU	Memoranda of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Person	Any individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision. (44 USC 3502)
Personally Identifiable Information (PII)	Information that directly identifies an individual. PII examples include name, address, social security number, or other identifying number or code, telephone number, and e- mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. Same as

	"information in an identifiable form". (ADS 508)
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Privacy Office
POA&M	Plan of Action and Milestones
Privacy Impact Assessment	An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, 2) to determine the risks and effects of collecting, [using,] maintaining and disseminating information in identifiable form in an electronic information system, and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (M-03-22)
Program Manager (PM)	Government official responsible and accountable for the conduct of a government program. A government program may be large (e.g., may provide U.S. assistance to other nations); it may also be a support activity such as the Agency's personnel or payroll program. (Chapters 508, 545, 552, 629)
SORN	System of Records Notice
SP	NIST Special Publication
SSN	Social Security Number
System	The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This term includes both automated and manual information systems. (ADS 508)
System Owner (SO)	Individual responsible for daily program and operational management of their specific USAID system. System Owners are responsible for ensuring that a security plan is prepared, implementing the plan and monitoring its effectiveness. (Chapters 508 and 545)
Third Country National (TCN) Employee	An individual who is 1) neither a U.S. citizen nor a permanent legal resident alien of the United States nor a host-country citizen, and 2) eligible for return travel to the home country or country of recruitment at U.S. Government expense.
Third-Party Web Sites or Applications	Web-based technologies that are not exclusively operated or controlled by a government entity. Often these technologies are located on a ".com" web site or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official web site.
USAID	United State Agency for International Development
USC	United States Code

6.2 APPENDIX B CONDUCTING THE PIA

6.2.1 Background

The E-Government Act mandates that all federal agencies conduct a Privacy Impact Assessment (PIA) when they use information technology (systems) to collect, use, maintain, or disseminate personally identifiable information (PII). PIAs provide information on how agencies handle PII, so that the American public has assurances that their PII is protected by their government.

The PIA is a risk-based analysis that enables USAID to determine the level of risk acceptable to the systems that support the conduct of USAID business functions. Risk mitigation helps USAID to 1) cost-effectively reduce information privacy risks to an acceptable level, 2) address information privacy throughout the life cycle of each system, and 3) ensure compliance with the federal authorities and USAID policies, procedures, and standards. The PIA's risk mitigation function works hand-in-hand with USAID's Certification and Accreditation (C&A), Security Controls Assessments (SCA), Risk Assessment, and Plan of Action and Milestones (POA&M) processes.

The PIA process should accomplish two goals: 1) determine the risks and effects of collecting, using, maintaining, and disseminating PII; and 2) evaluate protections and alternative processes for handling PII to mitigate potential privacy risks. The length and breadth of a PIA will vary by the size and complexity of the program or system. Any new system that involves the processing of PII should be able to demonstrate, through the PIA, that an in-depth analysis was conducted to ensure that privacy protections were built into the system.

This PIA Template is being used to gather information from program managers, system owners, and information system security officers. The information provided will be used by the Privacy Officer to analyze the privacy risks and controls for each system.

If you have questions about or would like assistance with this PIA Template, the PIA process, or other privacy compliance requirements please contact the USAID Privacy Office at privacy@usaid.gov.

6.2.2 Using this Word Template

This PIA form is a fillable Word template, which means that you can fill in the information in the appropriate fields, save the document, and submit the PIA electronically as an e-mail attachment. To create a PIA Word document from this PIA Template, use the following steps:

1. Click on **File** and then **Save As**.
2. In the **Save As** window save your PIA using the name provided; just update the date and version number with D for draft.
3. Then select **Word Document (*.docx)** from the **Save as type**: drop-down list.

6.2.3 Completing the PIA Template

This PIA Template has various fields to be completed. First, fill in or update the fields on the Title Page, Headers and Footers, and Change History Page.

- Fill in or edit, if appropriate, the Program Name and System Name sections on the title page. Update the Version number on the title page. The Approved date on the title page will be completed at the end of the process.
- Fill in the System Name field in the Header, and the Date field in the Footer. The date in the Footer should be the date you send this PIA to the Privacy Office for review.
- Update the Change History page to reflect your new version of this PIA. The date in the Change History should be the date you send this PIA to the Privacy Office for review.

Complete the contact information in Section 2: Contact Information and Approval Signatures. Insert the appropriate Name, Title, Office Name, Office Phone Number, and E-Mail address for the Program Manager, System Owner, and Information System Security Officer.

Continue to Section 3: Information, and answer the questions.

6.2.4 Answering the Questions

PIAs are formal documents and can be made available to the public on the USAID web site and upon request. Therefore, when completing this template, please respond to each question as if speaking to a member of the general public who is learning of this system for the first time.

- Each question has an answer box. Some answer boxes are simple text boxes, while other answer boxes have items to select, as appropriate.
- When you see a box (☐), you will be able to click on it to create a check mark to choose that item. Please select all items that apply. You should be able to add explanatory remarks in the answer boxes.
- Each section includes assistance (in blue text) on how to answer the question.
- Answer each question fully and completely. Answer each question with sufficient detail to permit the Privacy Office to analyze the privacy risks, controls, and risk mitigation plans.
- Type *Not Applicable* in the answer boxes for those questions that do not apply to your system and explain why the question is not applicable.
- Spell out each acronym the first time it is used in the PIA.
- Define technical terms or references, and keep in mind readers may not understand technical terms until they are explained.
- Use short and simple sentences.

- Use Spell Check and Grammar Check before submitting the PIA for approval.

6.2.5 Help Interpreting the Questions

Some questions provide choices, with the option to either pick one or pick all that apply. The questions that do not provide choices include explanations of the type of information that is required. At the end of each question, is a reference to the Privacy Controls, which provide more information on the topic. For more information on the Privacy Controls, please see Appendix D Privacy Controls.

6.3 APPENDIX C PRIVACY CONTROLS

Appendix J: Privacy Control Catalog in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013). To access *Appendix J*, use this link.

Table 5-3 Privacy Controls

ID	Privacy Controls
AP Authority and Purpose	Ensures that USAID identifies the legal bases that authorize a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected.
AP-1	Authority to Collect
AP-2	Purpose Specification
AR Accountability, Audit, and Risk Management	Enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that USAID is complying with applicable privacy protection requirements and minimizing overall privacy risk.
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI Data Quality and Integrity	Enhances public confidence that any PII collected and maintained by USAID is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.
DI-1	Data Quality
DI-2	Data Integrity and Date Integrity Board
DM Data Minimization and Retention	Helps USAID to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. USAID retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP Individual Participation and Redress	Addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in USAID decisions made based on the PII.
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE Security	Supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by USAID against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response

TR Transparency	Ensures that USAID provides public notice of its information practices and the privacy impact of its programs and activities.
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL Use Limitation	Ensures that USAID only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.
UL-1	Internal Use
UL-2	Information Sharing with Third Parties