MYUSAID Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
MYUSAID
Approved Date: February 7, 2017

Additional Privacy Compliance Documentation Required:

☐ None

☐ System of Records Notice (SORN)

☐ Open Data Privacy Analysis (ODPA)

☐ Privacy Act Section (e)(3) Statement or Notice (PA Notice)

☐ USAID Web Site Privacy Policy

☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents

☐ Role-Based Privacy Training Confirmation

Possible Additional Compliance Documentation Required:

☐ USAID Forms Management. ADS 505

☐ Information Collection Request (ICR). ADS 505, ADS 506, and ADS 508 Privacy Program

☐ Records Schedule Approved by the National Archives and Records Administration. ADS 502

Table of Contents

1 Introduction

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

2 Information

2.1 Program and System Information

2.1.1 Describe the PROGRAM and its PURPOSE.

USAID's MYUSAID is used to provide next generation Intranet capabilities, design processes, technology and content for USAID employee collaboration on projects and tasks. MYUSAID helps provide a more efficient and effective workplace for USAID employees working in multiple locations.

MYUSAID ensures USAID Intranet complies with:

- Executive Order 13576 – Delivering Efficient, Effective and Accountable Government
- Executive Order 13571 – Streamlining Service Delivery and Improving Customer Service
- USAID Agency Notice 04129 – Integration of Web Sites

MYUSAID provides a secure internal communication and data sharing medium for approximately 12,000 USAID employees. The intranet site includes bureau/office webpages, Agency documentation (i.e., guidelines, notices, directives), and access to social network collaboration tools such as blogs and team sites. MYUSAID acts as a repository of information for SUAID employees including policy, guidelines, Agency notices, directives and access. MYUSAID utilizes cloud based technology supplied by Huddle and Tibbr to improve collaboration and content management.

2.1.2 Describe the SYSTEM and its PURPOSE.

MyUSAID (IMI) is an integrated system that is architected using two cloud applications and an integration component:

• Huddle – SaaS content collaboration engine
• Tibbr – SaaS social collaboration engine
• Huddle for Tibbr app – Huddle and Tibbr integration

2.1.2 Describe the SYSTEM and its PURPOSE.

Tibbr: Tibbr provides USAID a secure and private enterprise social network that will facilitate social collaboration and knowledge sharing at work. It allows USAID employees to post news and updates, ask questions, make announcements, or share ideas with fellow USAID employees. Each USAID employee has a user profile on Tibbr that is searchable, providing USAID with an Agency-wide people directory and expert locator. Tibbr will enable USAID employees to easily share messages, polls, events, documents, and links with co-workers in Agency-wide and private contexts. Tibbr is organized around a Subject structure and users can create sub-subjects for an initiative, project, mission or Bureau. USAID employees will follow the subjects that they are interested in such as their Bureau or an initiative that they are working on in order to stay up to date on that topic. Users can create a private or public post to a subject or person, attach a file and have a discussion or ask a question.

The platform is available to any USAID employee around the globe with internet access both on their desktops and on mobile devices.

Huddle: Huddle is a collaboration platform that provides USAID with a secure environment where the Agency will manage, organize and work together on all of their content. Huddle workspaces are central repositories for all types of files to be saved and accessed by USAID offices around the globe. In workspaces, USAID users will manage project tasks, files and workflows. Huddle's file management features enable users to upload multiple files from their desktop, create a folder structure and share files with their team members through the platform. Users can share and comment on files, and direct the comments to specific team members. When edits to a file are required, users will open the file in its native application directly in the platform, make changes, and a new version will be automatically saved to the workspace. The editing feature provides users with all of the familiar features and functionality of the native application without leaving Huddle. Files are locked when they are opened for editing so there is no confusion about which user has made changes to a version. All content stored on Huddle has access permission settings so USAID can ensure that the right documents are visible and being shared with the appropriate users.

Workspaces provide a digital approval process which gives USAID an efficient and transparent document clearance tool. Clearances are achieved by requesting approval on a file and setting a deadline, and approval can be assigned to multiple people. Once approval is granted, the file is marked as approved by each individual and the action will appear in the activity feed.

The task feature in Huddle allows a user to assign, set a deadline and attach a file. With tasks, USAID can monitor a set of assignments for teams around their projects, while viewing a real-time stream of project actions. Tasks are tracked on each user's personalized dashboard which provides an overview of project activity and enables quick access to information about activity in all of a user's workspaces. All activity in Huddle is tracked and audited providing full transparency of the actions taken on a document or a project.

2.1.2 Describe the SYSTEM and its PURPOSE.

The platform is available to any USAID employee around the globe with internet access both on their desktops and on mobile devices.

Huddle for Tibbr app: The Huddle for Tibbr app integrates Huddle with Tibbr. It surfaces the rich Huddle document management features directly within Tibbr. USAID users can view, download, upload or share from Huddle using the Tibbr interface. Users are required to log in to Huddle so the permissions and access control to content persist across the platforms.

2.1.3 What is the SYSTEM STATUS?

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

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

- ☐ Physical only
- ☒ Electronic only
- ☐ Physical and electronic combined

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

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

2.1.6 What type of system and/or TECHNOLOGY is involved?
☐ Infrastructure System (Local Area Network, Wide Area Network, General Support System, etc.)
☒ Network
☒ Database
☒ Software
☒ Hardware
☒ Mobile Application or Platform
☐ Mobile Device Hardware (cameras, microphones, etc.)
☐ Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
☒ Wireless Network
☒ 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

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
☐ 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:
☐ None

2.2 Information Collection, Use, Maintenance, and Dissemination

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ Name, Former Name, or Alias
☐ 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

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☐ Patient Identification Number
☐ Employment or Salary Record
☐ Medical Record
☐ Criminal Record
☐ Military Record
☐ Financial Record
☒ Education Record
☐ Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
☐ 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:
☐ No PII is collected, used, maintained, or disseminated

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☒ Log Data (IP address, time, date, referrer site, browser type)
☒ Tracking Data (single- or multi-session cookies, beacons)
☒ Form Data
☒ User Names
☐ Passwords
☒ Unique Device Identifier
☒ Location or GPS Data
☐ Camera Controls (photo, video, videoconference)

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ Microphone Controls
☒ Other Hardware or Software Controls
☒ Photo Data
☒ Audio or Sound Data
☐ Other Device Sensor Controls or Data
☐ On/Off Status and Controls
☐ Cell Tower Records (logs, user location, time, date)
☒ Data Collected by Apps (itemize)
☐ Contact List and Directories
☐ Biometric Data or Related Data
☐ SD Card or Other Stored Data
☒ Network Status
☒ Network Communications Data
☐ Device Settings or Preferences (security, sharing, status)
☒ Other: Videos
☐ None

2.2.4 Who owns and/or controls the system involved?
☒ USAID Office: M/CIO
☐ Another Federal Agency:
☐ Contractor:
☒ Cloud Computing Services Provider: Huddle and Tibbr
☐ Third-Party Website or Application Services Provider:
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:

3 Privacy Risks and Controls

3.1 Authority and Purpose (AP)

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

The USAID Intranet system does not collect, use, maintain, or disseminate PII (including SSN information). No PII data should be imported into the USAID Intranet without the express approval by the individual.
IMI consists of two products (Tlbbr and Huddle). The risk of disseminating PII outside the USAID environment is limited as Tibbr is only accessible by users connected to the USAID network (including using SBC). Huddle is accessible from other devices, and does have a print feature.

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

PII is collected on direct-hires, foreign workers and contractors for the purpose of identification. Information such as names and telephone number may be used by the Human Resources and USAID Staff members for the purpose of finding experts and collaboration across the Agency.

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

Huddle and Tibbr are social and collaborative tools used to improve production and collaboration on USAID projects from different locations. Huddle and Tibbr may identify new ways to identify or notify USAID employees regarding work projects.

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

☐ No:

☒ Yes:

- ☐ Form or Survey (Please attach)
- ☐ OMB Number, if applicable:
- ☐ Privacy Act Statement (Please provide link or attach PA Statement)

3.2.3 Who owns and/or controls the personal information?
☒ USAID Office: M/CIO
☐Another Federal Agency:
☐ Contractor:
☒ Cloud Computing Services Provider:
☐ Third-Party Web Services Provider:
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:

3.2.8 Do you collect PII for an exclusively statistical purpose? If you do, how do you ensure that the PII is not disclosed or used inappropriately?
☒ No.
☐ Yes:

3.3 Data Quality and Integrity (DI)

3.3.1 How do you ensure that you collect PII to the greatest extent possible directly from the subject individual?
Any PII information collected and stored on the USAID Intranet systems are those collected directly from the individual and is assumed to be correct.

3.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?
The USAID Intranet will depend on their contractors, direct-hires and third-parties to verify their own personal information. In general it is left up to the individual to ensure that the information is accurate.

3.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?
USAID relies on contractors, direct-hires and third-party that have entered personal information into the USAID MYUSAID system to ensure accuracy.

3.4 Data Minimization and Retention (DM)

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

In order to conduct the SUAID mission the following PII information is collected: Name, Work Phone Number and Work email address. This information is used for normal business reasons for supporting collaboration.

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

☒ No.

☐ Yes:

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

MYUSAID does not produce reports about individuals based on the available PII information. Therefore no data anonymized data is necessary.

3.4.6 Does the system monitor or track individuals?

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

☐ No.

☒ Yes:

3.5 Individual Participation and Redress (IP)

3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?

All systems in the USAID Intranet infrastructure to which user input PII data have a mechanism were individuals can update their profile information and any other information stored about them. The PII collection is voluntary and is generally collected some type of web form. If the individual decides to decline or opt out then this information is not collected.

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

All individuals on the UISAID Intranet system have the opportunity to know what PII information is contained on the system about them. Individuals can generally access and correct the specific PII via a Helpdesk ticket to request correction or amendment, in addition to the USAID Freedom of Information Act (FOIA) and/or Privacy Act procedures under 22 CFR Part 215.

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

MYUSAID cloud service providers Huddle and Tibbr have provided administrative access to the specific applications. Information collected and stored in the cloud will be carefully monitored. Under the existing contract agreement with the cloud provider data can be made accessible for correction with written notification. Individuals can request access to and ament his/her personal information through the USAID Freedom of Information Act or Privacy Act request process.

3.7 Transparency (TR)

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

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

☐ No.

☒ Yes: Name and/or Work email address

3.7.2 How do you provide notice to individuals regarding?

1) The authority to collect PII:

2) The principal purposes for which the PII will be used:

3) The routine uses of the PII:

4) The effects on the individual, if any, of not providing all or any part of the PII:

The follow text is from the USAID intranet web-site privacy policy.

Privacy Policy

Thank you for visiting the USAID Intranet. Your privacy and security are very important to us. USAID does not collect personal information when you visit our website unless you choose to provide that information. However, we do collect some technical information about your visit to USAID.gov.

This is how we handle information about your visit to our Web site:

3.7.2 How do you provide notice to individuals regarding?

Information Collected and Stored Automatically

When you visit an USAID intranet website we may store some or all of the following:

- *the IP address from which you accessed our site*
- *the date and time*
- *the URL of the website from which you linked to our site the name of the file or words you searched for*
- *the pages you visited on our site the items clicked on a page*
- *the browser and operating system used*

We do not collect or track any personal information through these processes. We use this information, in the aggregate, to make our website more useful to visitors - to learn about the number of visitors to our site and the types of technology used, to detect operational problems, and to improve the website's overall security.

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

☒ No: We will update SORN 29 to include the update to IMI

☐ Yes:

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

For this project the cloud service providers Huddle and Tibbr has provided administrative access to the specific applications. Information collected and stored in the cloud will be carefully monitored. Under the existing contract agreement with the cloud provider data can be made accessible for correction with written notification. Individua ls can requests access to and amendment of his/her personal information through the USAID Freedom of Information Act or Privacy Act request process.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

The level of PII collected in the USAID Intranet solution is very small. Most of the information is accessible by USAID direct hires and contractors. It should be noted that all contractors with access to IT resources and data handling of personal information has been cleared to a Secret level. Both Huddle and Tibbr, the cloud service providers selected for this project, have employees that have been through the agencies required Background Investigation process and the agencies data will be stored on a FedRAMP certified infrastructure.

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

While there is no explicit sharing of PII information. During the course of normal business it is expected that PU data may be stored or transmitted to the cloud providers (Huddle and Tibbr) network. Also, there are cutTently no definitive plans on establishing connections outside USAID.

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

☒ No.

☐ Yes:

3.9 Third-Party Web Sites and Applications

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

While it is assumed that no deliberate transmission of Pll is anticipated, it is likely while using collaboration tools that PII information may be shared by users. The following list represents a listing of PII data used on the USAID Intranet system: Name, Work Phone Number, and Work E-Mail Address.

Appendix A. Links and Artifacts

A.1 Privacy Compliance Documents or Links

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