OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

USAID Needs to Improve Its Privacy Program to Better Ensure Protection of Personally Identifiable Information

AUDIT REPORT A-000-21-001-P
AUGUST 11, 2021

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, Millennium Challenge Corporation, U.S. African Development Foundation, and Inter-American Foundation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: August 11, 2021

TO: USAID, Bureau for Management, Chief Information Officer, Jay Mahanand

USAID, Bureau for Legislative and Public Affairs, Office of Web Management, Director, Gregory P. Your

FROM: Deputy Assistant Inspector General for Audit, Alvin Brown /s/

SUBJECT: USAID Needs to Improve Its Privacy Program to Better Ensure Protection of Personally Identifiable Information (A-000-21-001-P)

This memorandum transmits the final report on our audit of USAID's privacy program. Our audit objective was to assess the extent to which USAID has implemented key elements of an effective privacy program. Specifically, we assessed USAID's implementation of the following elements due to their importance in reducing the risk of inappropriate use or loss of personally identifiable information (PII): monitoring potential PII loss; providing role-based privacy training; reducing PII holdings, including Social Security numbers (SSNs); completing system of record notices (SORNs); and posting privacy notices. In finalizing the report, we considered your comments on the draft and included them in their entirety, excluding attachments, in Appendix E.

The report contains five recommendations to improve the effectiveness of USAID's privacy program. After reviewing information you provided in response to the draft report, we consider all five resolved but open pending completion of planned activities.

For all five recommendations, please provide evidence of final action to the Audit Performance and Compliance Division.

We appreciate the assistance you and your staff provided to us during this audit.

CONTENTS

INTRODUCTION

According to a 2020 IBM report, the average cost of a data breach is $3.86 million.[1] Moreover, that report states that 80 percent of security breaches included personally identifiable information (PII), more than any other compromised data type. Given an evolving cyber threat landscape and the number of cyberattacks on government agencies since 2014, effective protection of PII—such as Social Security numbers (SSNs) and birth dates—remains critical. In addition, due to the COVID-19 pandemic, USAID required most of its domestic staff to work from home. Working from home makes computer systems more vulnerable, increasing the risk of possible PII loss.

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. To mitigate risks of data breaches that threaten personal privacy, USAID needs to establish and maintain a robust privacy program aimed at protecting PII held by the Agency. A strong, multifaceted privacy program helps ensure that USAID considers privacy protections when making business decisions involving the collection, use, sharing, retention, disclosure, and destruction of PII, whether in paper or electronic form.

OIG initiated this audit after considering the risks associated with protecting PII. The audit objective was to assess the extent to which USAID has implemented key elements of an effective privacy program. Specifically, we assessed USAID's implementation of the following elements due to their importance in reducing the risk of inappropriate use or loss of PII: monitoring potential PII loss; providing role-based privacy training; reducing PII holdings, including SSNs; completing System of Records Notices (SORNs); and posting privacy notices.

To answer the audit objective, we assessed documentary evidence and controls related to USAID's data loss prevention (DLP) activities, role-based privacy training, SSN reduction plans, PII holdings, SORNs, and inventory of third-party websites. We also conducted interviews with USAID officials in Washington, DC, from the Privacy Office; the Bureau of Legislative and Public Affairs (LPA), Office of Web Management; and the Office of the Chief Information Officer (CIO). We conducted our work in accordance with generally accepted government auditing standards. Appendix A provides more details about our scope and methodology.

SUMMARY

USAID implemented some key elements of an effective privacy program, but additional controls are necessary to protect PII and reduce the risk of a privacy breach. For example, for the items tested, USAID justified the need to collect SSNs for systems in use, approved plans to protect PII, and published SORNs in the Federal Register. Yet USAID faced an increased risk of a breach and related financial loss because it had not

[1] International Business Machines, "Cost of a Data Breach Report 2020," , accessed January 21, 2021.

implemented other key privacy controls needed to protect PII and to provide the public with sufficient information about records containing their information. Specifically, USAID did not fully implement key controls related to:

- Preventing data loss because it did not have updated data loss procedures, including procedures to periodically review the DLP tool rules to assure that they were still effective.
- Providing role-based privacy training because the Agency's (1) process to validate who needed to take the training was not consistently followed nor documented and (2) policy did not require the training.
- Identifying actions needed to eliminate unnecessary SSNs because, according to a key Agency official, the Agency provided the information in annual metrics related to SSN reduction activities instead. However, the Agency still needs to update and implement its SSN reduction plan.
- Updating SORNs because its standard operating procedures (SOPs) were not updated to align with current requirements and the procedures were not complete.
- Tracking third-party websites accurately and completely because, according to Agency officials, it was not possible for them to know about all USAID third-party websites and the responsible official did not consider social media pages to be third-party websites.

We are making five recommendations to improve the effectiveness of USAID's privacy program. USAID agreed with four of our recommendations and partially agreed with one. Notwithstanding, the agency agreed to implement all five recommendations.

BACKGROUND

The Privacy Act of 1974, Public Law 93-579 (the Privacy Act) was enacted in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. The Privacy Act safeguards privacy by creating procedures and identifying substantive rights for personal data. It requires government agencies to show individuals any records kept on them and to follow certain principles when gathering and handling personal data. The Privacy Act also places restrictions on how agencies can share an individual's data with other agencies and allows individuals to bring a civil suit against the government for violating Privacy Act provisions. The following regulations provide additional guidance on how to handle privacy activities:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations" recommends privacy controls for Federal information systems and organizations, including role-based privacy training.

- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource" describes responsibilities for managing PII in Federal agencies.
- OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" discusses responsibilities for reviewing and eliminating unneeded PII holdings.
- OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act" discusses responsibilities for notifying the public about systems of records containing PII.
- NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" requires role-based training for individuals that have access to PII.
- "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics"[2] (April 17, 2020) provides reporting requirements for annual evaluations of the effectiveness of information security programs, including inventories of information systems.

In addition, USAID issued policies and procedures governing its privacy activities, including Automated Directives System (ADS), chapter 508, "Privacy Program," (July 30, 2019); "System of Records Notice (SORN) Standard Operating Procedures (SOP)," (April 1, 2019); and "Security Operations Center (SOC) Data Loss Prevention (DLP) Procedure" (February 16, 2016).

USAID is required to have an agency-wide privacy program that ensures compliance with applicable privacy requirements and manages privacy risks. USAID's CIO is responsible for the Agency's privacy program, and the Office of Website Management in LPA is responsible for the oversight of Agency third-party websites.

In October 2014, OIG issued "Audit of USAID's Implementation of Key Components of a Privacy Program for Its Information Technology Systems," which found that USAID did not implement key components of a privacy program—including policies and procedures, training, and monitoring for compliance. As of March 31, 2018, USAID closed all recommendations in that report.

USAID IMPLEMENTED SOME ELEMENTS OF AN EFFECTIVE PRIVACY PROGRAM, BUT ADDITIONAL KEY CONTROLS ARE NECESSARY TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION

We found that USAID implemented some elements of an effective privacy program, but additional key controls are needed. For the items tested, the Agency justified the need

[2] Published by OMB, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency.

to collect SSNs, held PII appropriately, and published SORNs. However, USAID did not fully implement key controls related to (1) implementing controls for DLP activities, (2) providing role-based privacy training, (3) preparing a comprehensive list of actions needed to eliminate unnecessary SSNs, (4) updating and fully completing SORNs, and (5) maintaining a comprehensive inventory of third-party websites.

USAID Implemented Some Elements of an Effective Privacy Program

For the items tested, we found that the Agency followed Federal privacy requirements to justify the need to collect SSNs for systems in use, had approved plans to protect PII, and published SORNs in the Federal Register.

OMB Circular A-130 requires agencies to take steps to eliminate unnecessary use of SSNs. Of a nonstatistical, randomly selected sample of 5 of the 18 USAID systems that collect SSNs, the Agency demonstrated that it had a bona fide need to collect SSNs.

USAID had approved plans to protect the PII in the systems tested. According to NIST SP 800-53, Rev. 4, agencies should "develop a security plan for the information systems" that is "approved by the authorizing official." We determined that a nonstatistical, randomly selected sample of 5 of the 32 USAID systems that held PII had security plans that were approved by the authorizing official. In addition, the three sampled systems that shared PII with other systems were authorized to share it.

Finally, the Agency published SORNs in the Federal Register. The Privacy Act defines a system of record as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying [information] assigned to the individual." OMB Circular A-108 requires each agency to publish SORNs in the Federal Register. The audit concluded that all 22 of USAID's SORNs on its list were published in the Federal Register as required.

USAID Lacked Controls for Data Loss Prevention Activities

USAID, however, did not fully implement some key privacy program controls necessary to protect PII, and additional actions are needed to address them. First, USAID did not fully document and implement DLP activities.

USAID's DLP tool did not prevent PII loss as required by Agency policy and responsible Agency staff did not always send warning notices to violators, as explained by the responsible Agency officials. The DLP tool did not prevent PII loss, as it did not capture emails with PII before they left the network. Google's DLP tool is a set of automated functions that monitor USAID's Gmail and Google Drive items for triggers to detect and prevent PII from being lost. Three days during audit fieldwork,[3] OIG sent a total of nine emails containing fillable PDF forms and Excel spreadsheets with fictitious PII,

[3] August 20, August 29, and September 3, 2020.

including SSNs, names, home addresses, email addresses, telephone numbers, and dates of birth. However, USAID's Google DLP tool did not capture those outgoing emails and prevent them from being sent.

According to ADS 508, the Agency's DLP tool is designed to prevent "non-encrypted emails containing PII" from leaving the network "by placing them in quarantine." According to Agency officials, Google DLP rules were weakened at the end of the prior fiscal year because changes were being made to Google Apps; however, after the changes were made, the rules were inadvertently not put back to their original settings. In addition, USAID did not have written procedures to periodically review the DLP rules to assure that they were still effective. Further, for email, Google DLP was configured to monitor for the loss of SSNs only; it did not monitor for other forms of PII, such as home addresses and dates of birth.

In addition to not capturing emails containing PII, warning notices were not always sent to violators. For a nonstatistical, randomly selected sample of 45 of the 426 Google DLP alerts of staff who attempted to send emails containing unencrypted SSNs outside the network, USAID could not provide evidence that a warning email was sent to one violator in accordance with the Agency's process.

According to USAID's "Security Operations Center (SOC) Data Loss Prevention (DLP) Procedure," when the DLP tool captures an email with PII, the email is quarantined, and a notice is sent to the violator. USAID's DLP team said that they were not aware of that procedure, and they were not following any other procedure. In addition, the procedure discussed a DLP tool that the Agency said it no longer used, instead of Google DLP. The procedure also did not discuss when violators should be notified of their captured DLP violations.

As a result, USAID had an increased risk of staff sending unencrypted PII, which elevates the risk of harm to individuals from inappropriate disclosure of their PII. It is important to note that even one PII breach can lead to litigation costs, compensation to the victims, and a lack of trust in the organization.

Not All Those Who Handled Personally Identifiable Information Completed Role-Based Training and Training Did Not Cover Some Key Topics

We found that some USAID staff did not take role-based privacy training and the training material did not include some privacy topics. Although everyone in the Agency who handles PII is required to receive annual role-based privacy training, only 6 of the 23 Travel Office staff who were required to take the training completed it. Further, 2 of the 213 staff from the Office of the Chief Financial Officer required to take the role-based privacy training did not complete the training.

In addition, USAID's role-based privacy training did not cover topics on identifying new privacy risks and retention schedules.[4] This occurred because USAID's "Information Technology (IT) Security Training—Policy, Standards, Guidelines, and Plan" primarily focuses on IT security and only mentions privacy role-based training. In addition, that plan did not delve into specific privacy topics required for role-based training.

NIST SP 800-53, Rev. 4, states that the organization should develop and implement "a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures." It further states that the organization should, at least annually, administer "targeted, role-based privacy training for personnel having responsibility for [PII]."

Although USAID had a process to validate its list of users that were required to take role-based privacy training, that process was not documented. Moreover, the process was not consistently followed, as USAID did not validate the list for the Travel Office in 2020. While USAID policy requires staff to attend annual general privacy training, it has not documented a similar requirement for role-based privacy training for staff whose duties include handling PII.

When an agency has a privacy breach, it must inform US-CERT.[5] From April 1, 2019, through March 31, 2020, USAID reported that 16 staff caused privacy-related US-CERT incidents. Of the 16 staff, 4 handled PII without taking required role-based privacy training.

By not ensuring that all required staff obtain role-based privacy training, USAID may not be making staff aware of their privacy responsibilities. As a result, Agency staff may not be equipped to effectively perform their assigned duties when handling PII. This increases the risk of inappropriate disclosure of PII and privacy breaches, which could lead to identity theft, loss of organization reputation, and litigation for misuse of PII.

USAID Did Not Identify Actions Needed to Eliminate Unnecessary Social Security Numbers

USAID issued its "2014 Implementation Plan and Progress Updates to Eliminate Unnecessary Use of SSNs" in August 2014, but the document did not contain plans to eliminate the unnecessary collection and use of SSNs as required. The plan only contained steps that the Agency would take to identify which systems and forms needed to be revised. However, the plan did not identify which systems and forms unnecessarily collected or used SSNs, and it did not identify actions needed or a target date to

[4] Identifying new privacy risks is discussed in NIST SP 800-53, Rev. 4. Retention schedules for PII are discussed in NIST SP 800-122.

[5] The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security. "US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities." Source: https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf.

eliminate those collections and uses. Further, the Agency did not prepare and publish its list of planned actions to eliminate unnecessary SSNs, which the 2014 document said would be completed by 2015.

According to OMB Memorandum M-07-16, agencies must establish a plan to eliminate the unnecessary collection and use of SSNs and provide annual updates on the progress of those plans. The Agency could not provide a reason as to why it had not fully implemented or updated the SSN reduction plan. According to a key official in USAID's Privacy Office, the Agency provided responses to annual metrics related to SSN reduction activities. However, those metrics did not provide specifics about updates and the implementation status of the plan. As a result, USAID did not have a roadmap to eliminate the unnecessary collection and use of SSNs, including the specific actions needed to reach that goal. Moreover, USAID risks continuing to unnecessarily collect, maintain, and use PII, which could result in the loss of sensitive information and reasonable litigation costs, as stated in the Privacy Act.

Some System of Record Notices Were Outdated and Others Were Missing Key Elements

OMB Circular A-108 requires each SORN to contain 26 elements to provide agency accountability to the public. However, of the 5 out of 22 SORNs selected nonstatistically at random, 3 SORNs had one outdated or missing element and 2 SORNs had 11 or more outdated or missing elements. For example, the SORN for USAID's Google Apps, a system that has been in operation at USAID for over 9 years, was missing a discussion of administrative, technical, and physical safeguards. However, USAID was aware that there were high risks when using Google Apps due to access and privacy control weaknesses. Not discussing the safeguards in the SORN was a significant omission because the public was left without relevant information about how the Agency would safeguard the PII that Google Apps stored.

Also, the "Congressional Relations, Inquiries, and Travel Records" and "Litigation Records" SORNs contained an incorrect address; thus, a user may not know how to contact the Agency to obtain and, if needed, correct their PII in the system. This change would warrant an updated SORN to make the public aware. Table 1 summarizes the number of outdated or missing elements for the five SORNs we sampled. See Appendix B for more details of the SORNs reviewed and the 26 SORN elements.

Table 1. USAID's Adherence to 26 Required Elements on 5 SORNs

	# of Acceptable Elements	# of Outdated Elements	# of Missing Elements	# of Elements Not Applicable[a]
Personnel Security and Suitability Investigations Records	24	1	0	1
Google Apps	24	0	1	1
Personal Services Contract Records	24	0	1	1
Congressional Relations, Inquiries, and Travel Records	14	2	9	1
Litigation Records	12	2	11	1

[a] USAID published only one version of the five SORNs selected, so there was no "History" on the SORNs. See Appendix B.
Source: OIG analysis of Agency SORNs.

According to OMB Circular A-108, "[a]gencies shall ensure that all SORNs remain accurate, up to date, and appropriately scoped . . . [and] that all SORNs are published in the Federal Register; that all SORNs include the information required by this Circular; and that all significant changes to SORNs have been reported to OMB and Congress." OMB Circular A-108 also states that "[a]gencies are required to publish a SORN in the Federal Register when . . . making significant changes to an existing system of records." OMB Circular A-108 goes on to explain that an example of a significant change is a "change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute (e.g., to seek access to or amendment of a record)."

Agency personnel stated that SORNs were last updated in 2016 and that they were in the process of updating the SORN for Google Apps and four other SORNs that were not part of this audit. Agency personnel also stated that they did not believe the other SORNs needed to be updated; in the Agency's opinion, the changes were not significant under OMB Circular A-108. However, OIG disagrees with the Agency's position and believes these changes are significant.

USAID officials knew about the new requirements found in that Circular. However, the Agency did not update its SORNs SOP, so personnel did not follow the new requirements. In addition, the SOP did not require the Agency to document instances where changes to the system were not significant enough to warrant an update to the SORN. Instead, the SOP stated that USAID reviews SORNs every 2 years, which aligned with old guidance in OMB Circular A-130 that was supplemented and clarified by

OMB Circular A-108 effective December 23, 2016. A key Agency official said that they were currently updating the SOP to align with the new guidance in OMB Circular A-108.

By not updating the Agency's SORNs, USAID provided the public and Agency staff with inaccurate information about how their PII is being stored, used, shared, and protected. The public and Agency staff need complete and accurate information, so individuals know how to contact the Agency to obtain and, if needed, correct their PII in the Agency's system.

USAID's Third-Party Websites Inventory Was Not Complete and Had Inaccurate Information

LPA did not maintain a complete and accurate inventory of public-facing websites, which includes those run by third parties. The inventory did not contain Uniform Resource Locations (URLs) for 202 of the 264 websites. The inventory also did not identify which websites collected PII. Furthermore, of the six nonstatistically selected websites that contained URLs[6], the inventory included four websites that the responsible Agency official explained were no longer used because projects ended. We also found that two of the websites collected PII. Finally, there were 23 third-party websites omitted from the Agency's third-party website inventory as of March 2020. See Appendix C for a list of errors in USAID's inventory of third-party websites.

OMB Circular A-130 states agencies shall "maintain an inventory of the agency's information systems that . . . collect . . . PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete." In addition, the "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics" (April 17, 2020) states that the organization should maintain "a comprehensive and accurate inventory of its information systems," including public-facing, third-party websites.

The third-party website inventory was inaccurate and incomplete because, according to LPA and CIO officials, it was not possible for them to know about all USAID third-party websites. Based on discussions with Agency officials, implementing partners and local entities may create or deactivate their own websites without notifying them. However, LPA is responsible for oversight of external Agency websites.[7] Also, the LPA official responsible for maintaining the inventory said that the 23 omitted websites are social media pages (e.g., Twitter, Facebook, and YouTube) and he did not consider social media pages to be third-party websites.

Without an accurate and complete inventory of third-party websites that make PII available to the Agency, USAID was unable to determine the extent to which privacy

[6] The websites were selected judgmentally to ensure the sample included foreign-based websites.
[7] ADS chapter 101, "Agency Programs and Functions," Jan 2021.

notices were placed on third-party websites and if additional privacy notices needed to be posted. As such, users may not have adequate information regarding how their PII would be protected and used by third-party websites.

CONCLUSION

While USAID implemented some key privacy controls to protect PII, additional actions are needed. USAID will continue to face an increased risk of a breach and related financial loss without having written procedures to help prevent data loss, revising privacy training standards, identifying actions needed to eliminate unnecessary SSNs and SORN procedures, and maintaining a current third-party website inventory. These key elements of a privacy program are needed to protect PII and provide the public with sufficient information about records containing their information so that they know how their PII is safeguarded against misuse. Acting now would also guard against loss, unauthorized use, and lack of trust in the organization and limit risks related to litigation and compensation to the victims.

RECOMMENDATIONS

We recommend that USAID's Chief Information Officer take the following actions:

1. Develop and implement written procedures to:
    - Periodically test the effectiveness of the rules for its data loss prevention tool and revise those rules when needed.
    - Configure the Agency's data loss prevention tool to prevent the loss of other types of personally identifiable information (such as home addresses and dates of birth), in addition to Social Security numbers.
    - Manage data loss prevention activities, including when staff should be notified of their violations.
2. Revise "Information Technology (IT) Security Training—Policy, Standards, Guidelines, and Plan" to document and implement a process for:
    - Providing role-based privacy training to staff that are responsible for processing personally identifiable information.
    - Providing role-based privacy training to staff at least annually.
    - Training staff on how to identify new privacy risks and retention schedules for personally identifiable information as required in the role-based privacy training materials.
3. Update and implement the Agency's Social Security number reduction plan.

4. Update and implement the Agency's "System of Records Notices Standard Operating Procedure" to:

   - Align with current requirements for reviewing and updating Agency system of record notices.
   - Document decisions that system changes were not significant and, thus, related system of record notices do not need to be updated.

   In addition, update the following system of record notices with the missing or incomplete elements identified in Appendix B of this document, as required by Office of Management and Budget Circular A-108:

   - Personnel Security and Suitability investigations records;
   - Google Apps;
   - Personal Services Contract records;
   - Congressional relations, inquiries, and travel records; and
   - Litigation records.

We also recommend that USAID's Bureau of Legislative and Public Affairs, Director of Web Management, take the following actions:

5. Develop and implement a plan to maintain a complete, accurate inventory of the Agency's third-party websites—including periodic reminders to staff that implementing partners should notify the Agency when creating or deactivating public-facing, third-party websites—and take action, where needed, to post privacy notices on websites that collect personally identifiable information.

OIG RESPONSE TO AGENCY COMMENTS

We provided our draft report to USAID on June 15, 2021. On July 21, 2021, we received the Agency's response which is included in Appendix E of this report.

The report included five recommendations. We consider all five resolved but open pending completion of planned activities.

We acknowledge management decisions on all five recommendations. USAID requested closure of recommendations 3, 4 and 5 upon report issuance. However, USAID did not provide sufficient evidence of its final action, and we did not agree to close them. Therefore, in subsequent correspondence, USAID provided target dates to complete its planned actions for recommendation 3 by July 15, 2022; recommendation 4 by January 20, 2022; and recommendation 5 by November 1, 2021.

In its response to recommendation 4, USAID said the system owner for the Personnel Security and Suitability investigations records confirmed that system location in the SORN is current. However, in subsequent correspondence, a responsible Agency official acknowledged that it was not and that it needs to be updated. As such, we did not make

a change in the audit report. Regarding outdated system location information, USAID said the Agency mailing address on its website remains current and that it also publishes the mailing and email addresses for the Agency's Chief Privacy Officer. However, the system location is required to be listed in the SORN. In response to the Agency comment, we did revise our report to state, "…thus, a user may not know how to contact the Agency to obtain and, if needed, correct their PII in the system."

APPENDIX A. SCOPE AND METHODOLOGY

We conducted this audit from March 12, 2020, through June 15, 2021, in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. In planning and performing the audit, we assessed and gained an understanding of internal controls that were significant to the audit objective. Specifically, we designed and conducted procedures related to 12 internal control principles under the 5 components of internal control as defined by the U.S. Government Accountability Office (GAO).[8] These included the Control Environment (principles 3-5), Risk Assessment (principles 7-9), Control Activities (principles 10-12), Information and Communication (principle 13), and Monitoring (principle 16-17). We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To develop the objective, we ranked and nonstatistically selected key recommendations from a 2014 OIG audit report[9] that, using our judgment, we believed represented the highest risks to the Agency's privacy program. See Appendix D for the full text of the key recommendations.

This audit was initiated to assess the state of USAID's privacy program in key areas to reduce the risk of inappropriate use or loss of PII. The audit objective was to assess the extent to which USAID has implemented key elements of an effective privacy program. Specifically, we assessed USAID's implementation of the following elements due to their importance in reducing the risk of inappropriate use or loss of PII: monitoring potential PII loss; providing role-based privacy training; reducing PII holdings, including SSNs; completing system of record notices (SORNs); and posting privacy notices.

The audit covered the period from April 1, 2019, to December 9, 2020, because we were reviewing the most recent control activities for the focus areas as of the date of the entrance conference. The fieldwork was performed remotely. Audit work covered USAID's Privacy Office in Washington, DC, and the Bureau of Legislative and Public Affairs (LPA), Office of Web Management located in Washington, DC, because those offices are responsible for handling the Agency's privacy activities and managing websites, respectively. In addition, we contacted USAID's Office of the Chief Financial Officer in Washington, DC, and the Travel Office in Washington, DC, as part of our efforts to validate the completeness and accuracy of their respective training records. We sought expert opinions from the OIG's Office of General Counsel. We also interviewed personnel and reviewed documentation to support our conclusions.

We selected samples where it was not practicable to assess 100 percent of the universe. We determined our sample sizes based on the frequency of the control. We selected a

[8] GAO, "Standards for Internal Control in the Federal Government," September 2014.
[9] USAID OIG, "Audit of USAID's Implementation of Key Components of a Privacy Program for Its Information Technology Systems" (A-000-15-001-P), October 10, 2014.

minimum sample size of 45 for large populations (i.e., more than 250 occurrences). We selected a minimum sample size of 10 percent of the population for medium populations (minimum 50 to 250 occurrences). For small populations (i.e., less than 50 occurrences), we selected a minimum sample size of 5 items. We used a random number generator to select the samples, except for third-party websites. We judgmentally selected third-party websites to ensure foreign-based websites were included in our sample selection. Due to the nature of sampling, we were unable to project the results of the samples to the entire universe of data or systems as applicable.

To answer our objective, we assessed the following six privacy control areas:

1. The extent to which USAID ensured that staff completed comprehensive role-based privacy training as required by USAID's plans and NIST SPs 800-53 (Rev. 4), 800-122, and 800-46 (Rev. 2).

We assessed whether USAID's privacy training plans addressed the areas identified in NIST SPs 800-53 (Rev. 4), 800-122, 800-46 (Rev. 2) and USAID's "Information Technology (IT) Security Training—Policy, Standards, Guidelines and Plan." We also reviewed the training materials and assessed the content to determine whether it satisfied those requirements. We compared lists of staff that were required to take role-based privacy training to those who took it to assess completeness. We also compared those lists to the Agency's staffing pattern to assess reliability of the Agency's list of staff required to take role-based privacy training. We reviewed Agency documents and inquired of Agency staff to determine whether USAID administered tests and established a threshold to confirm users' understanding of the privacy material.

2. The extent to which USAID implemented written procedures to review, update, and complete SORNs as required by OMB SORN guidance.

We obtained USAID's universe of 22 SORNs and reviewed a nonstatistically selected sample of 5 SORNs to determine whether they were published in the Federal Register, had all the required elements per OMB Circular A-108, and were updated based on auditor judgment.

3. The extent to which USAID's DLP tool and monitoring activities continuously identified and prevented the loss of PII as prescribed by NIST SP 800-122.

We used auditor judgment to determine whether USAID's DLP should monitor for the loss of more forms of PII, other than SSNs. We reviewed documentation to determine whether the DLP rules were configured to detect dates of birth, home addresses, and home phone numbers. We also conducted three blind tests by sending fictitious SSNs and other PII to personal email accounts using official USAID Google mail accounts and worked with the CIO team to determine whether the tool prevented or detected the losses. During a walkthrough meeting, we performed live testing where an Agency official sent emails with fictitious PII to the auditors' personal email accounts to determine whether the tool prevented or detected the losses. We reviewed DLP quarantine reports to determine whether the emails were captured by the tool. We assessed a nonstatistical sample of 45 out of 426 alerts from the DLP tool to determine whether authorized personnel received the alerts and assessed the actions taken by the

Agency for positive alerts. We also reviewed those 45 alerts to determine whether the violators completed their required privacy training and were given additional training if they had multiple violations.

4. The extent to which USAID developed and implemented its plan to eliminate the unnecessary use of SSNs as required by OMB Circular A-130.

We reviewed a nonstatistical sample of 5 out of 15 Agency-operated systems that collect PII (specifically SSNs) to determine whether the Agency required such information to conduct its business. Specifically, we interviewed Agency staff and reviewed supporting documentation to determine why the Agency needed SSNs and how the SSNs were collected and used. Based on that information, using auditor judgment, we determined whether SSNs were needed.

5. The extent to which USAID reviewed holdings of PII as required by OMB M-07-16.

We obtained USAID's PII holding review schedule to determine compliance with OMB M-07-16. We obtained the results of the last three annual reviews of PII holdings and, for a nonstatistical sample of 5 out of 32 Agency-operated systems that contained PII, reviewed supporting documentation to determine whether USAID reviewed its PII holdings. If we determined that the systems provided PII to other systems, we obtained additional documentation to determine whether those recipient systems were authorized to contain PII.

6. The extent to which USAID posted privacy notices on Agency third-party websites that collect PII as required by NIST SP 800-53.

We reviewed USAID's inventory of third-party websites for completeness by conducting internet searches to determine whether others should be included on the list. However, we could not rely on USAID's inventory of third-party websites because we identified concerns with its accuracy and completeness. We also reviewed the inventory to determine whether the list of 264 websites contained URLs for each website. We reviewed a nonstatistical sample of 6 of the 62 third-party Agency websites listed on the inventory that contained URLs to determine whether the websites contained privacy notices if PII was collected and whether the one that contained a notice contained all of the required elements identified in NIST SP 800-53, Rev. 4.

APPENDIX B. RESULTS OF SORNS REVIEW

Legend

✓ = SORN contained this information.

✓- = SORN contained this information, but it was not up to date.

X = SORN did not contain this information.

NA = This section was not applicable because there were no prior versions of these SORNs.

No.	OMB Circular A-108 Requirement	Personnel Security and Suitability Investigations Records	Google Apps	Personal Services Contracts Records	Congressional Relations, Inquiries, and Travel Records	Litigation Records
1	Agency	✓	✓	✓	✓	✓
2	Action	✓	✓	✓	X	X
3	Summary	✓	✓	✓	X	X
4	Dates	✓	✓	✓	X	X
5	Addresses	✓	✓	✓	X	X
6	For Further Information Contact	✓	✓	✓	X	X
7	Supplementary Information[a]	✓	✓	✓	X	X
8	System Name and Number	✓	✓	✓	X	X
9	Security Classification	✓	✓	X	X	✓
10	System Location	✓-	✓	✓	✓-	✓-
11	System Manager(s)	✓	✓	✓	✓-	✓-
12	Authority for Maintenance of the System	✓	✓	✓	✓	✓
13	Purpose(s) of the System	✓	✓	✓	✓	✓
14	Categories of Individuals Covered by the System	✓	✓	✓	✓	✓
15	Categories of Records in the System	✓	✓	✓	✓	✓
16	Record Source Categories	✓	✓	✓	✓	X
17	Routine Uses of Records Maintained in the System	✓	✓	✓	✓	✓

No.	OMB Circular A-108 Requirement	Personnel Security and Suitability Investigations Records	Google Apps	Personal Services Contracts Records	Congressional Relations, Inquiries, and Travel Records	Litigation Records
18	Policies and Practices for Storage of Records	✓	✓	✓	✓	✓
19	Policies and Practices for Retrieval of Records	✓	✓	✓	✓	✓
20	Policies and Practices for Retention and Disposal of Records	✓	✓	✓	✓	✓
21	Administrative, Technical, and Physical Safeguards	✓	X	✓	✓	✓
22	Record Access Procedures	✓	✓	✓	✓	X
23	Contesting Record Procedures	✓	✓	✓	✓	X
24	Notification Procedures[b]	✓	✓	✓	✓	X
25	Exemptions promulgated for the system	✓	✓	✓	X	✓
26	History[c]	NA	NA	NA	NA	NA

[a] Supplementary information is background information, including "a description of any changes being made to the system and the purpose(s) of the changes."

[b] Notification procedures explain how "an individual can be notified at his or her request if the system contains a record pertaining to him or her."

[c] History includes citation(s) "to the last full Federal Register notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision."

Source: OIG analysis of selected SORNs.

APPENDIX C. MISSING INFORMATION AND INACCURACIES IN USAID'S INVENTORY OF THIRD-PARTY WEBSITES

Below is the list of 23 third-party websites not included in the Agency's inventory:

1. https://www.facebook.com/USAIDSouthernAfrica
2. https://www.facebook.com/USAIDEgypt
3. https://twitter.com/USAIDEgypt
4. https://www.facebook.com/pages/USAID-Pakistan/440868732600680
5. https://twitter.com/USAID_Pakistan
6. https://www.facebook.com/USAIDGhana
7. http://www.youtube.com/user/usaiddakar
8. https://www.facebook.com/USAIDSenegal
9. https://twitter.com/USAIDES
10. http://www.youtube.com/USAIDElSalvador
11. https://twitter.com/USAID_Colombia
12. http://www.youtube.com/user/USAIDColombiaVideo
13. https://www.facebook.com/usaid.philippines
14. https://twitter.com/USAID_Manila
15. https://www.facebook.com/usaidindonesia
16. http://www.flickr.com/people/usaid-indonesia/
17. https://twitter.com/usaidindonesia
18. https://www.facebook.com/USAIDUkraine/info
19. https://www.facebook.com/USAIDGeorgiaHealthCareImprovementProject
20. https://www.facebook.com/USAIDGeorgia
21. http://www.youtube.com/user/USAIDGeorgia
22. https://twitter.com/USAIDGeorgia
23. https://www.facebook.com/USAIDSouthSudan/

The following are the four third-party websites that USAID stated should not have been included in the inventory: (1) http://uniter.org.ua; (2) http://capla.asia/index.php/en/; (3) http://thekaizencompany.com/(collects PII); and (4) http://www.nigerianextt.org/ (collects PII).

APPENDIX D. SELECTED FINDINGS AND RECOMMENDATIONS FROM THE 2014 AUDIT REPORT

Finding	Recommendation
USAID Did Not Fully Provide Role-Based Privacy Training	8. Develop and implement documented role-based privacy training for the following employees: security staff, human resources staff, contracting officers' staff, financial officers' staff, chief information security office staff, and travel staff.
USAID Did Not Complete System of Record Notices (SORN)	12. Develop and implement written procedures to review and update SORNs on at least a biennial basis.
USAID Did Not Monitor Data Loss Prevention Tool Continuously for Potential Loss of Personally Identifiable Information	18. Make a written risk-based determination of the frequency that the data loss prevention tool and Pretty Good Privacy should be monitored, and based on that determination, implement appropriate corrective actions and document the results.
USAID Did Not Fully Develop and Implement Plan to Eliminate Unnecessary Use of Social Security Numbers	19. Revise its written plan to eliminate the unnecessary collection and use of Social Security numbers, to include time frames for reviewing and eliminating the unnecessary collection and use of partial and full Social Security numbers in Agency forms and systems. 20. Implement its plan to eliminate the unnecessary collection and use of Social Security numbers, and document the results.
USAID Did Not Review Holdings of Personally Identifiable Information Regularly	21. Develop and implement documented procedures for reviewing the Agency's PII holdings.
USAID Did Not Post Privacy Notices on Its Third-Party Web Sites	24. Develop and implement a written process to review the Agency's inventory of third-party Web sites periodically for completeness and prepare and post privacy notices on the Web sites wherever the public might make PII available to the Agency.

Source: OIG, "Audit of USAID's Implementation of Key Components of a Privacy Program for Its Information Technology Systems" (Report No. A-000-15-001-P), October 10, 2014.

APPENDIX E. AGENCY COMMENTS

MEMORANDUM

TO: IG/A/ITA Director, Lisa Banks

FROM: Bureau of Management, Chief Information Officer, Jay Mahanand /S/

DATE: July 21, 2021

SUBJECT: Management Comments to Respond to the Draft Audit Report Produced by the Office of Inspector General (OIG) titled, "USAID Needs To Improve Its Privacy Program To Better Ensure Protection of Personally Identifiable Information." (A-000-21-00X-P, AA100620)

The U.S. Agency for International Development (USAID) would like to thank the Office of Inspector General (OIG) for the opportunity to provide comments on the subject draft report. The Agency agrees fully, or, in part with the five recommendation(s). We appreciate the comments in your report and believe they align with the improvements we already have planned or are underway.

USAID understands the importance of conducting proper oversight to ensure consistent compliance with federal privacy requirements. We also recognize the importance of effectively implementing privacy enabling technologies to mitigate the impact of privacy incidents and promote increased transparency into the Agency's collection and safeguarding of personally identifiable information in our systems. Recognizing that a breach of sensitive personally identifiable information (PII), such as social security numbers, could result in substantial harm or unfairness to individuals, USAID prioritizes the protection of sensitive PII to mitigate privacy impacts.

USAID has made significant progress in establishing a comprehensive framework to administer its privacy program, since the most recent OIG audit conducted in 2014. The 2014 OIG Report identified 34 compliance issues related to privacy protection laws, regulations, policies, and training. Since that time, the Privacy Program:

- Developed and implemented policies and guidance for assessing the privacy impacts of IT systems and programs that involve PII. The Privacy Program has developed detailed guidance and templates to standardize the preparation of Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), and System of Records Notice (SORN).
- Developed and implemented a robust plan for responding to privacy incidents.
- Provides ongoing privacy awareness training to USAID employees and contractors;
- Developed and implemented procedures for reviewing new and existing information collections for unnecessary use of SSNs.
- Participated in various Working Groups to increase privacy awareness and foster a culture of privacy stewardship across the Agency.
- Developed and implemented guidance and templates for drafting Privacy Act Statements and Notices to facilitate compliance with the Privacy Act's notice requirements.

Despite these significant gains, there is still much work to be done. USAID is committed to doing the work. Since the conclusion of this audit, USAID has taken affirmative measures to review and enhance the controls in our Data Loss Prevention Tool to more effectively screen and restrict the unsecured email transmission of PII. We developed four modules of role-based privacy training. USAID developed and implemented an updated Social Security Number Reduction Plan. USAID launched an initiative to review and update its SORN inventory and coordinated with system owners to review and initiate the modification of outdated SORNs. We are pleased to report that the Agency published a Modified System of Records Notice for USAID-27: Partner Vetting System as recently as January 2021. In addition, USAID developed a process to capture websites as they are conceived and developed and has updated ADS-557 outlining said process.

Attached find our plans for implementing the recommendations, and reports on significant progress already made.

We look forward to working with you again in the future to continuously make improvements to the privacy program.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE REPORT RELEASED BY THE USAID OFFICE OF THE INSPECTOR GENERAL (OIG) TITLED, USAID Needs To Improve Its Privacy Program To Better Ensure Protection of Personally Identifiable Information (A-000-21-00X-P)

Please find below the management comments from the U.S. Agency for International Development (USAID) on the draft report produced by the Office of the USAID Inspector General (OIG), which contains 5 recommendations for USAID:

Recommendation 1: We recommend that USAID's Chief Information Officer take the following actions:

Develop and implement written procedures to:

- Periodically test the effectiveness of the rules for its data loss prevention tool and revise those rules when needed.
- Configure the Agency's data loss prevention tool to prevent the loss of other types of personally identifiable information (such as home addresses and dates of birth), in addition to Social Security numbers.
- Manage data loss prevention activities, including when staff should be notified of their violations.

Management Comments: USAID agrees with this recommendation. USAID DLP is currently configured to look for ALL instances of SSN.[10] USAID developed and implemented procedures that require bi-weekly testing of the existing rules and procedures for updating Google LLC in the event updates are required. USAID has also developed written procedures to manage data loss prevention activities that include instructions and guidelines for alerting staff of confirmed violations.[11] USAID agrees to establish new screening rules to look for other sensitive forms of PII, including financial

[10] USAID explored options for configuring a rule to screen for home addresses (and telephone numbers) that would not significantly impede business processes. At this time, it is impractical to implement such a rule using the automated tool. However, USAID will continue to work to identify options for increasing the effectiveness of the DLP screening controls.

[11] See Data Loss Prevention Job Aid_ Google DLP Test Harness SOP and the RACI: Alert Procedure for Native Google DLP Security Application.

account information, passport information, and driver's license numbers, as well as targeted standard forms that collect PII. USAID is committed to monitoring and improving the effectiveness of its DLP tool to ensure that it is operating as intended.[12]

Target Completion Date: December 1, 2021 (See attached **"Artifacts"** supporting documentation for Rec 1)

Recommendation 2: We recommend that USAID's Chief Information Officer take the following actions:

Revise "Information Technology (IT) Security Training—Policy, Standards, Guidelines, and Plan" to document and implement a process for:

- Providing role-based privacy training to staff that are responsible for processing personally identifiable information.
- Providing role-based privacy training to staff at least annually.
- Training staff on how to identify new privacy risks and retention schedules for personally identifiable information as required in the role-based privacy training materials.

Management Comments: USAID agrees with this recommendation. USAID Automated Directive Systems Chapter 508: Privacy Program requires that the Chief Information Officer (CIO) provide targeted, role-based training a minimum of once annually to those members of the workforce having responsibility for PII or for activities that involve PII.[13] While CIO has implemented an Agency-wide privacy-training program and develops and delivers a variety of ongoing, ad-hoc, remedial and role-based training to individuals that handle PII and diverse stakeholders, USAID agrees that a better process to document and monitor the completion of role-based training is necessary. Therefore, the CIO will work closely with the identified points of contact from applicable USAID offices (SEC, CFO, HCTM, and Travel) to: (i) identify the appropriate staff that are responsible for processing personally identifiable information; (ii) implement a process for: providing role-based training to staff that are responsible for processing PII; (iii) provide role-based privacy training to staff annually, and (iv) train staff on how to identify new privacy risks as required in the role-based privacy training

[12] USAID notes, however, that Google LLC regularly enhances functionality and adds product features. These changes are assessed by a 3rd Party Assessor Organization for FedRAMP. USAID is not always provided notice when such changes are implemented. In 2018, Privacy recommended that the Google contracts/agreements be amended to require notice of any changes that involve the processing of PII to mitigate the potential privacy impact. See Google Services PIA.

[13] ADS Chapter 508 Section 508.3.5.6.

materials.[14] This process will be described in the training plan and procedures documentation and verifiable through training reports within the USAID Learning Management System (LMS).

Target Completion Date: August 31, 2021 (See attached **"Artifacts"** supporting documentation for Rec 2)

Recommendation 3: We recommend that USAID's Chief Information Officer take the following actions:

Update and implement the Agency's Social Security number reduction plan.

Management Comments: Agree. USAID supports government-wide efforts to reduce the use of the Social Security Number (SSN) and acknowledges that our progress toward achieving this aim is difficult to measure without a documented SSN Reduction Plan. As a result of this engagement, USAID updated its Social Security Number Collection and Use Policy. The Policy will be submitted to Cyberscope as part of USAID's Annual FISMA Report.

Although the Agency continues to rely on SSNs for important government programs and shared services that rely on the use of the SSN as a common identifier to ensure they are matching their information to the correct records in another entity's systems, like employment, background investigations, payroll, tax reporting and benefits administration, USAID has developed and implemented effective procedures for documenting its justification for using SSNs.[15] USAID has already taken steps to implement the SSN Reduction Plan. USAID established a SSN Use and Reduction Working Group in December 2020. USAID deployed an automated solution for screening email traffic for SSNs and blocking the numbers' transmittal to external, non-government users when an SSN is detected. While this solution was tailored specifically to address the Agency's SSN Reduction Plan, USAID also leveraged already existing information security and privacy management processes and procedures to review the collection, use and disclosure of SSNs and to ensure that SSNs are protected when stored in agency information systems. Specifically:

- USAID uses existing processes for conducting privacy impact assessments to determine whether a new collection, use or disclosure of SSNs is necessary to achieve the Agency's mission. See Appendix D of the PTA/PIA Template.

[14] USAID developed role-based training that provides additional guidance for consulting with the appropriate official (Information Records Division) to establish retention schedules as required by ADS-502: The USAID Records Management Program (Travel Privacy Role-based Training 20210524, see slide # 42). See also HCTM Role-Based Training 20210524 and ISSO Privacy and Security Training 20201103.

[15] See OIG findings on page 3 of this report: "{f}or the items tested, the Agency justified the need to collect SSNs {and} held PII appropriately."

- Similarly, USAID uses existing processes for reviewing proposed new information collections to track and monitor any new collections that involve SSNs to confirm and document that planned collections of SSNs are appropriate and authorized.[16]
- USAID policy requires encryption of all sensitive personally identifiable information, including SSNs, transmitted via email. It also restricts access to SSNs based on need-to-know and least-privilege principles.[17] ADS 508 provides explicit guidance to address rare circumstances in which SSNs must be sent via U.S. mail. USAID staff are required to ensure that SSNs are not visible on the outside of any mail, double-wrapping pages that contain SSN, and follow specific instructions for mailing SSNs to posts abroad.[18]
- USAID conducts an annual data call, Annual Records and Personally Identifiable Information (PII) Inventory as required by the 21st century digital record-keeping requirements and OMB A-130 requirement to maintain a PII Holdings Inventory.[19] The SSN Use and Reduction Working Group will continue exploring options for reducing the Agency's collection and use SSNs to the maximum extent practicable.
- USAID developed targeted, role-based training for workforce members with significant privacy responsibilities, or who manage activities that involve the collection and processing of SSNs and other sensitive PII.[20]

Target Completion Date: USAID requests closure of the recommendation upon the OIG's issuance of a Final Report. (See attached **"Artifacts"** supporting documentation for Rec 3)

Recommendation 4: We recommend that USAID's Chief Information Officer take the following actions:
Update and implement the Agency's "System of Records Notices Standard Operating Procedure" to:

1. Align with current requirements for reviewing and updating the Agency system of record notices.

[16] See Forms Review Tracker.

[17] ADS-545mbd: Rules of Behavior for Users. See sections 2,6, and 7.

[18] See Section 3.8.3 and USAID Notices Restriction on Social Security Numbers on Documents Sent by U.S. Mail FINAL 10-23-2018.

[19] See 2020-PII Inventory.

[20] See SSN Use Collection Training.

2. Document decisions that system changes were not significant and, thus, related system of record notices do not need to be updated.

In addition, update the following system of record notices with the missing or incomplete elements identified in appendix B of this document, as required by Office of Management and Budget Circular A-108:

1. Personnel Security and Suitability investigations records;
2. Google Apps;
3. Personal Services Contract records;
4. Congressional relations, inquiries, and travel records; and
5. Litigation Records.

Management Comments: Partially Agree. USAID acknowledges the intent of this recommendation and acknowledges its responsibility to ensure that all SORNs remain accurate, up-to date, and appropriately scoped; and that all SORNs published in the Federal Register include the information required by OMB Circular A-108: Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act. As a result of this engagement, USAID has taken steps to improve its policies and procedures that govern periodic reviews of SORN documentation to better support our statutory and regulatory privacy obligations.

USAID disagrees, however, with the framing of this recommendation, noting that USAID policy does not authorize the CIO to take unilateral action to publish or maintain SORNs. The Privacy Program's compliance management process begins when system owners, program managers, and/or system of records managers prepare a PTA or PIA and submits it to the Privacy Program for review. Under ADS Chapter 508, program managers, system owners and system of records managers are responsible and accountable for ensuring the accuracy and currency of privacy documentation and compliance with federal privacy authorities.[21]

Under the guidance of the Chief Privacy Officer, the Privacy Program implements USAID's privacy continuous monitoring activities, which include PTA, PIA and SORN review and approval. The Chief Information Officer and the USAID Privacy Program rely on the system owners, program manager and system of records owner to report when a new information collection is planned and when significant changes are made to an existing system that require a notice of a modified system of records.

Decisions regarding whether system changes warrant a SORN update are documented during the PTA and PIA processes. During both the PTA and PIA review process, system owners, in consultation with the Privacy Program, document system changes and determine whether a system change requires modification of a prior PTA/PIA, whether

[21] See Sections 508.2(p)(q)(r) and 508.3.11.2.

a new SORN is required, or an existing SORN continues to cover the program or system.[22] USAID uses the Privacy Program's "New or Modified SORN Template (SORN Template)" to provide detailed instructions for drafting a SORN. The SORN Template contains all elements required by OMB A-108.

The SORN SOP referenced in the recommendation is an internal resource used to facilitate Privacy Program's staff review and approval of SORNs routed by system owners/program managers. It also describes the required actions to initiate the OMB authorization process, notify Congress, publish the SORN in the Federal Register and post it on **www.usaid.gov**.[23] It is not intended for agency-wide use.[24] Nonetheless, USAID embraced the opportunity to improve the Privacy Program's SORN SOP to document procedures for periodic review of published SORNs and includes specific instructions for documenting decisions related to system changes that do not require updates to the SORN.[25]

USAID fully supports the intent of this recommendation and is committed to improving its coordination with system owners to ensure increased compliance with federal laws and policies that mandate the accuracy, timeliness, and completeness of SORNs. USAID has taken actions to enhance transparency into the handling and safeguarding of PII. The Privacy Program notified system owners of the missing and/or outdated SORN elements identified in this report and initiated additional measures, such as drafting updated SORNs, to ensure the prioritization of activities required to effectively remediate the deficiencies identified in Appendix B.[26] USAID published a Modified System of Records Notice for USAID-27: Partner Vetting System as recently as January 2021. 86 FR 3109, January 14, 2021, and we look forward to completing a comprehensive review of our SORN inventory to bring them in alignment with Privacy Act and OMB reporting requirements.

However, USAID disagrees with one deficiency identified in Appendix B and the characterization of the privacy impacts related to the SORN deficiencies identified in the report.

- USAID 08: Personnel Security and Suitability Investigations Records - Appendix B

[22] Questions 10 and 11 in the PTA/PIA Template solicit information with the specific intent of determining if a SORN is required and provide notice informing the SO/SM that a SORN is required in the event of a positive response.

[23] The Privacy Program publishes the notice on usaid.gov. System Owners publish any required Notices of Proposed Rulemaking related to the SORN in the Federal Register as required by ADS Chapter 156: Federal Rulemaking (ADS-156).

[24] *See* ADS-508, Section 508.3.11.2.

[25] See Section 3.1.

[26] See SORN Coordination Emails.

lists the system location element as out of date. The system owner confirmed that the address listed in the published SORN is current.[27]

- The report finds that the outdated system location information in USAID 22: Congressional Relations, Inquiries and Travel Records and USAID 26 - Litigation Records would result in a user's inability to contact the Agency to request access and correct PII maintained in USAID systems. USAID publishes its privacy policies, including standard procedures for submitting Privacy Act requests at usaid.gov/privacy. Additionally, USAID successfully migrated the enterprise data center to a hybrid cloud solution. USAID now uses multiple data centers' hosting systems, services, applications, and storage without relying on any particular geographic location. The mailing address on USAID's website remains current. USAID also publishes the mailing and email addresses for the Agency's Chief Privacy Officer.
- USAID 30: Google Apps Records -- USAID agrees with the deficiencies identified. In fact, the Google Services PIA was updated in 2018, at which time, the Privacy Program documented required updates to the SORN as a POA&M.[28] The OIG report notes that, as a result of the deficiencies, the public was left without relevant information about how the Agency would safeguard PII stored by Google Apps. Although not published in the Federal Register, USAID publishes its privacy policies, including how it safeguards PII it collects and maintains in its systems, including the Google Services PIA, at usaid.gov/privacy. Additionally, the original version of the Google Services PIA published on the Agency's website contained a section entitled "Information Security," which notified the public of safeguards to protect the integrity and security of PII collected by Google Apps.

The Privacy Program also proposed changes to ADS 508 to promote enhanced continuous privacy compliance monitoring and enable increased coordination, guidance, review and approval of SORNs.[29]

The proposed policy revision clarifies system owner responsibilities for drafting and submitting all required privacy compliance documentation to the Privacy Program for review and approval. It requires use of the Privacy Program's SORN template to publish and modify SORNS. The proposed draft also requires system owners to implement continuous monitoring procedures to document changes to the system of records and codifies existing practices that leverage the Privacy Impact Assessment annual

[27] See 2021.06.01 - USAID Mail-USAID 8 SORN Review Status.

[28] See Google Services PIA_20180918, Section 3.7.3.

[29] See ADS-508 Proposed Revision, Section 508.2(e).

compliance monitoring process as an additional opportunity to identify whether changes to an information system trigger the necessity to publish and/or update a SORN. The proposed revision includes requirements for documenting whether the changes are significant and a rationale for determining that a change is not significant. It explicitly states that significant changes trigger the requirement to publish a Modified System of Records Notice.[30] The proposed revision contains standards for identifying significant changes/updates that may trigger a SORN requirement; and, thus require the Chief Privacy Officer's review and approval.[31]

The Privacy Program has achieved considerable progress in this area as a result of this audit and the trend is continuing.

Target Completion Date: USAID requests closure of the recommendation upon the OIG's issuance of a Final Report. Prior to the initiation of this evaluation, the Privacy Program developed a SORN Template, which contained instructions aligned with current OMB requirements for reviewing and updating Agency system of record notices. The Template is incorporated into agency policy as a mandatory reference to ADS-508. As a result of this engagement, the Privacy Program updated the SORN SOP and spearheaded the initiative to address the deficiencies identified in Appendix B. Additionally, the Privacy Program recommended changes to USAID's Agency-wide Privacy policy to facilitate increased oversight and greater coordination in the development and maintenance of privacy compliance documentation. (See attached **"Artifacts"** supporting documentation for Rec 4)

Recommendation 5: We also recommend that USAID's Bureau of Legislative and Public Affairs, Director of Web Management develop and implement a plan to maintain a complete, accurate inventory of the Agency's third-party websites—including periodic reminders to staff that implementing partners should notify the Agency when creating or deactivating public-facing third-party websites.

Management Comments: USAID agrees with this recommendation. The Director of Web Management, Bureau of Legislative and Public Affairs (LPA), working closely with M/CIO/IT Operations, has developed a process to capture websites as they are conceived and developed, and has updated ADS 557 outlining said process. The resulting inventory will be available on demand on the Agency's intranet. Additionally, as the definition of a third-party website has been expanded to include social media platforms, LPA has conducted an updated call for review of the Agency's registry of social media sites hosted on the U.S. Digital Registry at digital.gov as required by *OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services*. This call, completed in January 2020, is now an annual requirement for responsible staff to review the Agency's records for accuracy and will be included in upcoming training for Agency communicators.

[30] Id. Section 508.3.4.5.5.

[31] Id. Section 508.3.4.3.

Target Completion Date: USAID requests closure of the recommendation upon the OIG's issuance of a Final Report. (See attached **"Artifacts"** supporting documentation for Rec 5)

In view of the above, we request that the OIG inform USAID when it agrees or disagrees with a management comment.

APPENDIX F. MAJOR CONTRIBUTORS TO THIS REPORT

The following people were major contributors to this report: Mark S. Norman, audit director; Lisa M. Banks, assistant director; Felix Adenusi, lead auditor; Joanne Howard, senior counsel; Modupe A. Demuren, auditor; Christopher D. Marotta, auditor; and Wangui Kiundi, writer-editor.