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

USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA

Audit Report No. A-000-23-004-C
September 8, 2023

Information Technology Audits Division

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

MEMORANDUM

DATE: September 8, 2023

TO: USAID, Chief Information Officer, Jason Gray

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

SUBJECT: USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA (A-000-23-004-C)

Enclosed is the final audit report on USAID's information security program for fiscal year (FY) 2023, in support of the Federal Information Security Modernization Act of 2014 (FISMA).[1] The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the audit. The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on USAID's compliance with FISMA. CLA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which CLA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USAID implemented an effective information security program.[2] To answer the audit objective, CLA assessed the effectiveness of USAID's implementation of the FY 2023 IG FISMA reporting metrics[3] that fall into the nine domains in the following table. Also, CLA assessed USAID's implementation of selected management,

[1] Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 5274, which amends the Inspector General Act of 1978, when USAID OIG contracts with an audit firm to perform the work, USAID OIG provides non-governmental organizations and/or business entities specifically identified in the accompanying report, if any, 30 days from the date of report publication to review the final report and submit a written response to USAID OIG that clarifies or provides additional context for each instance within the report in which the non-governmental organization and/or business entity is specifically identified. Any comments received to this effect are posted for public viewing on https://usaid.oig.gov with USAID OIG's final transmittal. Please direct related inquiries to oignotice_ndaa5274@usaid.gov.

[2] For this audit, an effective information security program was defined as having an overall mature program based on the current year inspector general FISMA reporting metrics.

[3] Office of Management and Budget and Council of the Inspectors General on Integrity and Efficiency, "FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," February 10, 2023.

technical, and operational controls outlined in NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," December 10, 2020.

CLA reviewed 6 of 72 judgmentally selected systems in USAID's inventory as of October 7, 2022. Audit fieldwork covered USAID's headquarters located in Washington, DC, and included 10 overseas missions for certain tests. It covered the period from October 1, 2022, through June 22, 2023.

CLA concluded that USAID generally implemented an effective information security program. For example, USAID:

- Maintained an effective configuration management program.
- Implemented an effective mobile device management program.
- Maintained an effective information system continuous monitoring program.

However, as summarized in the table below, CLA found weaknesses in four of the nine FY2023 IG FISMA metric domains.

Fiscal Year 2023 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	X
Supply Chain Risk Management	
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	X
Contingency Planning	

To address the weaknesses identified in the report, we recommend that USAID's Chief Information Officer take the following actions:

Recommendation 1. Formally document and implement a revised policy for maintaining a system component inventory to include the specific physical location of hardware assets.

Recommendation 2. Fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.

In addition, USAID took corrective action to close two of four open recommendations from the FY2020[4] and FY2021[5] FISMA audits. Refer to Appendix III on page 14 of CLA's report for the status of prior year recommendations.

In finalizing the report, the audit firm evaluated USAID's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. For recommendations 1 and 2, please evidence of final action to the Audit Performance and Compliance Division.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

[4] Recommendation 6 in USAID OIG, "USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA" (A-000-21-004-C), January 7, 2021.
[5] Recommendation 2 in USAID OIG, "USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA" (A-000-22-005-C), December 7, 2021.

United States Agency for International Development
Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2023

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

Director, Information Technology Audits Division
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the United States Agency for International Development's (USAID) information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual review of their agencies' information security program and report the results to the Office of Management and Budget (OMB).

The objective of this performance audit was to determine whether USAID implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2023 IG FISMA reporting metrics).

For this year's review, OMB required IGs to assess 20 core and 20 supplemental IG FISMA reporting metrics in the following five security function areas to assess the maturity level and the effectiveness of their agencies' information security program: Identify, Protect, Detect, Respond, and Recover.[1] The maturity levels ranging from lowest to highest are: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. According to the FY 2023 IG FISMA reporting metrics, Managed and Measurable and Optimized are considered effective maturity levels.

The audit included an assessment of USAID's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope included assessing selected security controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA reporting metrics for a sample for a sample of 6 of 72 internal and external systems in USAID's FISMA inventory of information systems.

Audit fieldwork covered USAID's headquarters located in Washington, DC, from December 1, 2022, to June 22, 2023. In addition, the following overseas missions were included in three of our samples: Philippines, Honduras, Georgia, Ethiopia, Peru, Kenya, South Sudan, Nigeria, Bangladesh, and Uganda. It covered the period from October 1, 2022, through June 22, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[1] The function areas are further broken down into nine domains.

We concluded that USAID implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2023 IG FISMA reporting metrics. Although we concluded that USAID implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted two weaknesses and made two new recommendations to assist USAID in strengthening its information security program. In addition, two recommendations from prior FISMA audits remain open.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our audit to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from USAID on or before September 8, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 8, 2023.

The purpose of this audit report is to report on our assessment of USAID's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to the USAID Office of Inspector General.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
September 8, 2023

Table of Contents

SUMMARY OF RESULTS

Background

The United States Agency for International Development (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[2] (FISMA) requirement for an annual evaluation of the USAID's information security program and practices. The objective of this performance audit was to determine whether USAID implemented an effective information security program.[3]

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

FISMA also requires Agency Inspectors General (IGs) to assess the effectiveness of Agency information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

OMB and the Council of the Inspectors General on Integrity and Efficiency annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA reporting metrics[4] to independently assess their agencies' information security program.

[2] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of OMB with respect to Agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[3] For this audit, an effective information security program was defined as having an overall mature program based on the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2023 IG FISMA reporting metrics).

[4] We submitted our responses to the FY 2023 IG FISMA reporting metrics to USAID OIG as a separate deliverable under the contract for this audit.

For fiscal year (FY) 2023, OMB required IGs to assess the 20 core and 20 supplemental Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program. As highlighted in Table 1, the FY 2023 IG FISMA reporting metrics are designed to assess the maturity of the information security program and align with the five function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2023 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For this audit, we reviewed selected controls[5] mapped to the FY 2023 IG FISMA reporting metrics for a sample of 6 of 72 USAID internal and external information systems[6] in USAID's FISMA inventory as of October 7, 2022.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

We concluded that USAID implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2023 IG FISMA reporting metrics. For example, USAID:

- Maintained an effective configuration management program.
- Implemented an effective mobile device management program.
- Maintained an effective information system continuous monitoring program.

Table 2 below shows a summary of the overall maturity levels for each domain and function area in the FY 2023 IG FISMA reporting metrics.

[5] The controls were tested to the extent necessary to determine whether USAID implemented the processes specifically addressed in the IG FISMA reporting metrics. In addition, not all controls were tested for all six sampled information systems since several controls were inherited from USAID's general support system and certain controls were not applicable for external systems.

[6] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Table 2: Maturity Levels for the FY 2023 IG FISMA Reporting Metrics

Security Function	FY 2023 Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Managed and Measurable	**Risk Management**	Managed and Measurable
		Supply Chain Risk Management	Optimized
Protect	Consistently Implemented	**Configuration Management**	Managed and Measurable
		Identity and Access Management	Managed and Measurable
		Data Protection and Privacy	Managed and Measurable
		Security Training	Consistently Implemented
Detect	Optimized	**Information Security Continuous Monitoring**	Optimized
Respond	Managed and Measurable	**Incident Response**	Managed and Measurable
Recover	Managed and Measurable	**Contingency Planning**	Managed and Measurable
Overall	**Level 4: Managed and Measurable - Effective**		

Although we concluded that USAID implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted one weakness in the risk management and configuration management domains and another weakness in the identity and access management and the incident response domains. (See Table 3.) Therefore, we made two new recommendations to assist USAID in strengthening its information security program. In addition, USAID took corrective action to close two of four open recommendations from prior FISMA audits.[7] [8]

Table 3: Weaknesses Noted in the FY 2023 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2023 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	USAID Needs to Strengthen its Inventory Management Process **(See Finding # 1)**
	Supply Chain Risk Management	None
Protect	**Configuration Management**	USAID Needs to Strengthen its Inventory Management Process **(See Finding # 1)**
	Identity and Access Management	USAID Needs to Strengthen its Event Logging Capabilities **(See Finding # 2)**

[7] *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-000-21-004-C, January 7, 2021).

[8] *USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-000-22-005-C, December 7, 2021).

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metrics Domain	Weaknesses Noted
	Data Protection and Privacy	None
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	USAID Needs to Strengthen its Event Logging Capabilities **(See Finding # 2)**
Recover	**Contingency Planning**	None

In response to the draft FISMA report, USAID agreed with and outlined its plans to address the two recommendations. We acknowledge management's decision on recommendations 1 and 2. Further, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. USAID's comments are included in their entirety in Appendix II.

The following section provides a detailed discussion of the audit findings. Appendix I describes the audit scope and methodology.

AUDIT FINDINGS

1. USAID NEEDS TO STRENGTHEN ITS INVENTORY MANAGEMENT PROCESS

Cybersecurity Framework Security Function: *Identify and Protect*
FY 2023 IG FISMA Reporting Metric Domain: *Risk Management and Configuration Management*

NIST Special Publication (SP) 800-53, Revision 5, security control CM-8, System Component Inventory, states the following regarding inventory management:

a. Develop and document an inventory of system components that:
…
   4. Is at the level of granularity deemed necessary for tracking and reporting; and
   5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability].

In addition, USAID Automated Directives System Chapter 545, Section 545.3.6.8, states:

System Owners must:
…
d. Ensure the hardware inventory is at the level of granularity deemed necessary for tracking and reporting. The inventory specifications include:

   1. Vendor/manufacturer name;
   2. Hardware model number, item description, and serial number; and
   3. Physical location of hardware.

USAID did not consistently document the physical location of assets in the hardware inventory at a level of granularity deemed necessary for tracking and reporting as required by NIST and agency policy. Specifically, USAID did not maintain granular detail of the physical location for 712 of 87,637 information technology assets in the hardware inventory. For example, the building name in Washington, DC or the Mission location was listed in the inventory, but not the specific location, such as the room or office number. Management stated that the granularity of location was not consistently documented for all items in the hardware inventory due to the lack of specificity required in the policy. Further, CLA observed that the policy did not require the specific location, such as the office or room number, to be included in the inventory.

Unspecific inventories may lead to stolen or misplaced IT equipment, resulting in an increased risk of loss of control of USAID data, including personally identifiable information. This may also cause a strain on the Agency's budget as unplanned or unnecessary spending may be required to replace stolen or misplaced computing equipment. Therefore, we are making the following recommendation.

> ***Recommendation 1:*** *We recommend that USAID's Chief Information Officer document and implement a revised policy for maintaining a system component inventory to include the specific physical location of agency hardware assets.*

2. USAID NEEDS TO STRENGTHEN ITS EVENT LOGGING CAPABILITIES

Cybersecurity Framework Security Function: *Protect and Respond*
FY 2023 IG FISMA Reporting Metric Domain: *Identity and Access Management and Incident Response*

OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, addresses the logging requirements in the Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021). That memorandum establishes a maturity model to guide the implementation of requirements across event logging tiers as shown below that are designed to help agencies prioritize their efforts and resources to achieve full compliance with requirements for implementation, log categories, and centralized access. In addition, the memorandum requires that agencies forward all required event logs, in a near real-time automated basis, to centralized systems responsible for security information and event management.[9] Requirements for OMB's event logging maturity model are summarized in the table below.

Table 4: Event Logging Maturity Model

OMB M-21-32 Event Logging Maturity Level	Requirements
Event Logging 1 Tier, Rating - Basic (to be met by August 27, 2022)	• Basic Logging Categories • Minimum Logging Data • Time Standard • Event Forwarding • Protecting and Validating Log Information • Passive DNS • Cybersecurity Infrastructure Security Agency and Federal Bureau of Investigations Access Requirements • Logging Orchestration, Automation, and Response – Planning • User Behavior Monitoring – Planning • Basic Centralized Access
Event Logging 2 Tier - Intermediate (to be met by February 26, 2023)	• Meeting EL1 maturity level • Intermediate Logging Categories • Publication of Standardized Log Structure • Inspection of Encrypted Data • Intermediate Centralized Access

Source: Auditor generated based on OMB Memorandum M-21-31.

[9] Security information and event management (SIEM) tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components. SIEM tools automate the collection of event log records from tools and report them to a management console in a standardized format. SIEM tools facilitate correlation and analysis. The correlation of logs with all components of an organization's network and business applications provides additional tools that may assist in determining the veracity and scope of potential attacks.

USAID did not fully implement event logging tiers 1 and 2, as required by OMB M-21-31. Instead, USAID's maturity was at tier 0, as the Agency's did not meet or only partially met the highest criticality logging requirements. As such, the Agency's event logging capabilities were not effective.

USAID management stated they rely on third parties to implement the required logging services; however, third parties' logging enhancements were not implemented for all the Agency's systems. USAID management also stated the Agency is performing due diligence in capturing all OMB M-21-31 compliance requirements through careful vendor selection while executing continuous improvement of log ingestion in a reasonable and prudent manner. Management further stated that the Agency issued a contract dedicated to this effort in October 2022 and implementation is in progress.

Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud services providers) is invaluable in the detection, investigation, and remediation of cyber threats. However, USAID did not have the ability to correlate event logs across different repositories in a complete or risk-based manner, which increased the risk that the Agency may not collect all meaningful relevant data on suspicious events. Moreover, USAID may inadvertently miss the potential scope or veracity of suspicious events or attacks. Therefore, we are making the following recommendation.

> ***Recommendation 2:*** *We recommend that USAID's Chief Information Officer fully implement event logging requirements in accordance with Office of Management and Budget Memorandum M-21-31.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft FISMA report, USAID agreed with and outlined its plans to address the two recommendations. We acknowledge management's decision on recommendations 1 and 2. Further, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. USAID's comments are included in their entirety in Appendix II.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to determine whether USAID implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the current IG FISMA reporting metrics.

Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The scope of this performance audit was to assess USAID's information security program consistent with FISMA and reporting instructions issued by the OMB and the Council of the Inspectors General on Integrity and Efficiency. In accordance with those instructions, we assessed 20 core metrics and 20 supplemental metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA reporting metrics for a sample of 6 of 72 internal and external information systems in USAID's FISMA inventory as of October 7, 2022.

In addition, we performed an internal vulnerability assessment of USAID's network. The audit also included a follow up on prior FISMA audit recommendations[10] [11] to determine whether USAID made progress in implementing them. See Appendix III for the status of the prior recommendations.

Audit fieldwork was conducted at USAID's headquarters located in Washington, DC, from December 1, 2022, to June 22, 2023. In addition, the following overseas missions were included in three of our samples: Philippines, Honduras, Georgia, Ethiopia, Peru, Kenya, South Sudan, Nigeria, Bangladesh, and Uganda. It covered the period from October 1, 2022, through June 22, 2023.

[10] Recommendations 2, 3, and 6 in *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-000-21-004-C, January 7, 2021).

[11] Recommendation 2 in *USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-000-22-005-C, December 7, 2021).

Methodology

To determine if USAID implemented an effective information security program, CLA conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, CLA reviewed documents supporting the information security program. These documents included, but were not limited to, USAID's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, CLA compared documents, such as USAID's information technology policies and procedures, to requirements stipulated in Executive Order 14028, relevant OMB memorandums, and NIST special publications. CLA also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, CLA reviewed the status of FISMA audit recommendations from fiscal years 2020[12] and 2021.[13] See Appendix III for the status of prior year recommendations.

In assessing the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. CLA considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, CLA considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, based on risk, significance, or criticality this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

To perform our audit of USAID's information security program and practices, CLA followed a work plan based on, but not limited to, the following guidance:

- *Government Auditing Standards* (April 2021).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022).
- Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities.*
- FY 2023 IG FISMA Reporting Metrics (February 10, 2023).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls (December 10, 2020).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of security control effectiveness.

[12] Ibid 7.

[13] Ibid 8.

- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy,* for the risk management framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (February 2014).
- USAID policies and procedures.

MANAGEMENT COMMENTS

MEMORANDUM

TO: Deputy Assistant Inspector General for Audit, Alvin Brown

FROM: USAID Chief Information Officer, Jason Gray M/CIO /s/

DATE: August 11, 2023

SUBJECT: Management Comments to Respond to the Draft Audit Report Produced by the Office of Inspector General titled, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA (Task no.* AA150522*)*

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 with the recommendations, herein provides plans for implementing them, and reports on significant progress already made.

USAID is committed to supporting improvements to managing our information security program as required by the Federal Information Security Modernization Act of 2014 (FISMA). The OIG acknowledges this commitment in the draft report, by recognizing that our agency had generally implemented an effective agency-wide information security program in Fiscal Year 2023.

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 GENERALLY IMPLEMENTED AN EFFECTIVE INFORMATION SECURITY PROGRAM FOR FISCAL YEAR 2023 IN SUPPORT OF FISMA (Task no.* AA150522*)*

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 two recommendations for USAID:

Recommendation 1: Formally document and implement a revised policy for maintaining a system component inventory to include the specific physical location of hardware assets.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will formally document and implement a revised policy for maintaining the Agency hardware inventory to include requiring the specific physical location of hardware assets to the degree possible.

- **Target Completion Date:** August 31, 2024.

Recommendation 2: Fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will fully implement event logging (EL) requirements in accordance with Office of Management and Budget, Memorandum M-21-31 with the top focus being an overall improved security posture.

- **Target Completion Date:** December 31, 2023.

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

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2020 and FY 2021[14] FISMA audit recommendations.

No.	FY 2020 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
2	USAID's Chief Information Officer should collaborate with the Office of Human Capital and Talent Management to document and implement a process to verify that separated employees' accounts are disabled in a timely manner in accordance with USAID policy.	Open	Agree
3	USAID's Chief Human Capitol Officer should implement a process to maintain records electronically for onboarding and off boarding staff.	Open	Agree
6	USAID's Chief Information Officer develop and implement a process to block unauthorized applications from installing on Agency mobile devices.	Open	Closed Although USAID did not submit a closure memo to the USAID OIG, based on the testing performed for the FY 2023 FISMA audit, CLA determined the recommendation is closed.

No.	FY 2021 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
2	USAID's Chief Information Officer should address the management of system components requiring repair or service in its Supply Chain Risk Management Standard Operating Procedures.	Closed	Agree

[14] Ibid 7 and 8.