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

USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA

Audit Report A-000-22-005-C
December 7, 2021

Information Technology Audits Division

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

MEMORANDUM

DATE: December 7, 2021

TO: USAID, Chief Information Officer, Jay Mahanand

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

SUBJECT: USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-000-22-005-C)

Enclosed is the final audit report on USAID's information security program for fiscal year (FY) 2021, in support of the Federal Information Security Modernization Act of 2014 (FISMA). 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.[1] To answer the audit objective, CLA evaluated the effectiveness of USAID's implementation of the "FY 2021 Inspector General FISMA Reporting Metrics"[2] that fall into the nine domains in the following table. Also, CLA assessed USAID's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." CLA reviewed 6 of the 52 information systems in USAID's inventory as of February 12, 2021. Audit fieldwork covered USAID's headquarters located in Washington, DC,

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

[2] Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," May 12, 2021.

and included 15 overseas missions for certain tests. Fieldwork was performed from October 1, 2020, through September 2, 2021, and covered the period from October 1, 2020, through September 2, 2021.

The audit firm concluded that USAID implemented an effective information security program. For example, USAID:

- Improved its vulnerability management program.
- Maintained an effective incident response program.
- Maintained an effective contingency planning and disaster recovery program.

However, as summarized in the table below, CLA noted weaknesses in four of the nine FY 2021 IG FISMA metric domains.

Fiscal Year 2021 **IG FISMA Metric Domains**	**Weaknesses** **Identified**
Risk Management	X
Supply Chain Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	

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

Recommendation 1. Implement a process to automatically disable system user accounts after 90 days of inactivity or implement a daily review process to ensure that accounts are disabled after 90 days of inactivity.

Recommendation 2. Address the management of system components requiring repair or service in its Supply Chain Risk Management Standard Operating Procedures.

In addition, USAID had not taken final action on three recommendations from the FY 2020 FISMA audit.[3] Refer to Appendix III on page 17 of CLA's report for the status of prior year recommendations.

[3] Recommendations 2, 3, and 6 in USAID OIG, "USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA" (Audit Report A-000-21-004-C), January 7, 2021.

In finalizing the report, the audit firm evaluated USAID's responses to the recommendations. After reviewing that evaluation, we consider recommendation 1 closed and recommendation 2 resolved but open pending completion of planned activities. For recommendation 2, please provide 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.

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

Fiscal Year 2021

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

December 2, 2021

Ms. Lisa Banks
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Ms. Banks:

CliftonLarsonAllen LLP (CLA) is pleased to present our final report on the results of our audit of the United States Agency for International Development's (USAID) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2021.

We appreciate the assistance we received from USAID. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

Inspector General
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 2021 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 current year IG FISMA reporting metrics.

For this year's review, OMB required IGs to assess 66 metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The audit included an assessment of USAID's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope also included assessing selected security controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 6 of 52 internal and external systems in USAID's FISMA inventory of information systems.

Audit fieldwork covered USAID's headquarters located in Washington, DC. In addition, the following overseas missions were included in two of our samples: Bangladesh, Ghana, Haiti, Kenya, Madagascar, Mozambique, Nicaragua, Nigeria, Republic of Guatemala, Rwanda, Senegal, Sri Lanka, South Africa, Thailand, and Uganda. Fieldwork was conducted from April 9, 2021, to September 2, 2021. It covered the period from October 1, 2020, through September 2, 2021.

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.

We concluded that USAID implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2021 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 five weaknesses that fell in the risk management, supply chain risk management, configuration management, and identity and access management domains of the FY 2021 IG FISMA reporting metrics and have made two new recommendations to assist USAID in strengthening its information security program. In addition, we noted three recommendations in a prior FISMA audit 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 performance 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 December 2, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to December 2, 2021.

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
December 2, 2021

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[1] (FISMA) requirement for an annual evaluation of the U.S Agency for International Development's (USAID) information security program and practices. The objective of this performance audit was to determine whether USAID implemented an effective information security program.[2]

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 Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 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[3] to independently assess their agencies' information security program.

[1] 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.

[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year Inspector General (IG) FISMA reporting metrics.

[3] We submitted our responses to the FY 2021 IG FISMA reporting metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

As highlighted in Table 1, the fiscal year (FY) 2021 IG FISMA reporting metrics are designed to assess the maturity[4] 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. The FY 2021 IG FISMA reporting metrics include Supply Chain Risk Management (SCRM), a new domain within the Identify function area; however, the SCRM domain was not considered in the Identify framework function rating.

For FY 2021, OMB required IGs to assess 66 metrics in the five security function areas to determine the effectiveness of their information security program and the maturity level of each function area.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 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 2021 IG FISMA reporting metrics for a sample of 6 of 52 USAID internal and external information systems[6] in USAID's FISMA inventory as of February 12, 2021.

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.

[4] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized. To be considered effective, an agency's information security program must be rated *Managed and Measurable* (Level 4).

[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 the USAID 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.

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 2021 IG FISMA reporting metrics.[7] For example, USAID:

- Improved its vulnerability management program.
- Maintained an effective incident response program.
- Maintained an effective contingency planning and disaster recovery program.

Table 2 below shows a summary of the overall maturity levels for each domain and function area in the FY 2021 IG FISMA reporting metrics.

Table 2: Maturity Levels for the FY 2021 FISMA Reporting Metrics

Security Function	FY 2021 Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Managed and Measurable	**Risk Management**	Managed and Measurable
		Supply Chain Risk Management	Ad Hoc[8]
Protect	Managed and Measurable	**Configuration Management**	Managed and Measurable
		Identity and Access Management	Managed and Measurable
		Data Protection and Privacy	Managed and Measurable
		Security Training	Managed and Measurable
Detect	Managed and Measurable	**Information Security Continuous Monitoring**	Managed and Measurable
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 five weaknesses that fell in the risk management, supply chain risk management, configuration management, and identity and access management domains of the FY 2021

[7] In accordance with the FY 2021 FISMA reporting metrics, ratings throughout the nine domains were determined by a simple majority, where the most frequent level across the metrics served as the domain rating. Agencies were rated at the higher level in instances when two or more levels were the most frequently rated. The domain ratings inform the overall function ratings, and the five function ratings inform the overall agency rating.

[8] The FY 2021 IG FISMA reporting metrics indicated that, to provide agencies with sufficient time to fully implement NIST Special Publication 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore would not be considered for the overall rating.

IG FISMA Metrics (see Table 3) and have made two new recommendations to assist USAID in strengthening its information security program. In addition, we noted three recommendations in a prior year FISMA audit are still open.[9]

Table 3: Weaknesses Noted in the FY 2021 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	USAID Needs to Strengthen Its Inventory Management Process **(See Finding # 4)** USAID Needs to Strengthen Mobile Device Management Controls **(See Finding # 5)**
	Supply Chain Risk Management	USAID Needs to Enhance Its Supply Chain Risk Management Procedures **(See Finding # 3)**
Protect	**Configuration Management**	USAID Needs to Strengthen Configuration Management Controls **(See Finding # 2)**
	Identity and Access Management	USAID Needs to Strengthen Account Management Controls **(See Finding # 1)**
	Data Protection and Privacy	None[10]
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

[9] Refer to Appendix III for the status of prior year recommendations.

[10] Although our testing of the 6 sampled systems did not identify weaknesses in the USAID privacy program, a recent OIG audit report identified certain weaknesses related to USAID's inventory of personally identifiable information, systems of records notices, and reviews of Social Security numbers. See USAID OIG's audit report: "USAID Needs to Improve Its Privacy Program to Better Ensure Protection of Personally Identifiable Information" (A-000-21-001-P, August 21, 2021).

In addition, USAID took corrective action to close 6 recommendations from the FY 2018,[11] FY 2019,[12] and FY 2020[13] FISMA audit reports. Refer to Appendix III for the status of prior year recommendations.

In response to the draft FISMA report, USAID agreed with the two recommendations. USAID stated they completed final action and requested closure of recommendation 1 upon issuance of the final report. Based on our evaluation of the Agency's comments and review of the evidence provided, we agree that recommendation 1 is closed. USAID also outlined its plans to address recommendation 2. We acknowledge management's decision on recommendation 2, and, therefore, consider recommendation 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.

[11] *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).

[12] *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-000-20-005-C, February 7, 2020).

[13] *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).

AUDIT FINDINGS

1. USAID NEEDS TO STRENGTHEN ACCOUNT MANAGEMENT CONTROLS

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Identity and Access Management*

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security control AC-2, Account Management, states the following regarding managing information system accounts:

> The Organization:
>
> ***
>
> e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts.
>
> Control Enhancements:
>
> ***
>
> 3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

Also, security control PS-4, Personnel Termination, states the following regarding managing information system accounts for terminated employees:

> The Organization:
>
> a. Disables information system access within [Assignment: organization-defined time-period].

Further, security control PS-6, Access Agreements, states the following regarding access agreements:

> The Organization:
>
> ***
>
> c. Ensures that individuals requiring access to organizational information and information systems:
>
> 1. Sign appropriate access agreements prior to being granted access.

In addition, USAID ADS Chapter 545*, Information Systems Security*, states the following regarding account management and access agreements controls:

- Approvals by system Information System Security Officers and System Owners designees are required for requests to create information system accounts and authorize access to the information system based on a valid access authorization.
- System Owners must configure the information system to automatically disable accounts after 90 days of inactivity.
- Ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

In addition, the *USAID Master Common Controls Catalog version 1.4*, requires the disablement of information system access within two weeks of termination.

USAID did not effectively manage user accounts for two of six sampled systems. Specifically, the following was identified for one system:

- Accounts for 16 from a total population of 226 separated employees were not disabled. Management stated that, although the employees were listed as separated on the report provided, the individuals were still active employees. However, USAID's Office of Human Capital and Talent Management and Office of Acquisition and Assistance did not provide evidence to validate their employment status.
- For a sample of 25 new hires from the total population of 319 new hires, evidence was not provided for 5 users to validate that their access was approved and for 6 users to validate whether access agreements were signed prior to gaining system access. According to USAID management, many of the documents could not be provided because they were available only in hard copies, not electronically.

Additionally, for a second system, the following was identified:

- One privileged and five non-privileged users remained active past 90 days of inactivity and were not disabled in accordance with the 90-day inactivity requirement. Management stated that the accounts were not disabled due to an oversight during the bi-annual account review process. However, a bi-annual review process is not sufficient to identify accounts requiring disablement after 90 days of inactivity. In addition, an automated control was not implemented for disabling inactive accounts. Upon notification of this issue, management disabled the accounts.

Without ensuring accounts are disabled due to inactivity or separation, USAID is at an increased risk of account misuse and access. In addition, without ensuring system access is approved and documented, USAID is at an increased risk of individuals being granted inappropriate access to systems and/or roles and permissions. Further, without ensuring new information system users complete access agreements prior to gaining system access, there is an increased risk that system users do not understand their responsibilities when accessing USAID's information systems and managing USAID data.

Recommendations were made in the FY 2020 FISMA audit report[14] regarding account disablement for separated employees and retention methods for access approval forms and agreements. Because USAID had not taken action to fully address those recommendations, we are not making new recommendations at this time. However, we are making the following recommendation to address the automatic disablement of accounts.

[14] Recommendations 2 and 3, *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).

> ***Recommendation 1:*** *We recommend that USAID's Chief Information Officer implement a process to automatically disable system user accounts after 90 days of inactivity. If automatic disabling of accounts is not possible, we recommend the USAID's Chief Information Officer implement a daily review process to ensure that accounts are disabled after 90 days of inactivity.*

2. USAID NEEDS TO STRENGTHEN CONFIGURATION MANAGEMENT CONTROLS

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Configuration Management*

NIST SP 800-53, Revision 4, security control CM-3, Configuration Change Control, states the following regarding change management:

> The organization:
>
> 1) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.

We were unable to validate whether a security impact analysis (SIA) was completed, and changes were approved by the Change Control Board (CCB) for the entire population of two sampled changes for one system due to lack of evidence provided.

Management stated that the *Configuration Management Plan* was based on a generic template and was not reflective of the operating environment for changes made to the system. Upon identification of the issue, we validated that management updated the *Configuration Management Plan* to reflect that a SIA and CCB approval are required for major changes. In addition, per management, the operating environment does not require CCB approval for changes that do not impact infrastructure or architecture.

Without conducting security risk analysis and obtaining approvals for changes in the USAID environment, USAID is at risk of being unaware of the security impact and risks caused by changes to its information system environment. Since USAID revised the requirements in the *Change Management Plan* for the specific issues noted, we are not making a recommendation at this time.

3. USAID NEEDS TO ENHANCE ITS SUPPLY CHAIN RISK MANAGEMENT PROCEDURES

Cybersecurity Framework Security Function: *Identify*
FY 2021 FISMA IG Metric Domain: *Supply Chain Risk Management*

Public law 115-390 – 115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* or the ''SECURE Technology Act" (December 31, 2018) requires executive agencies to develop an overall SCRM strategy and implementation plan and policies and processes to guide and govern SCRM activities.

Also, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* states, "organizations should include in their anti-counterfeit policy and procedures, a means to help ensure that the components acquired and used are authentic and have not been subject to tampering."

In addition, NIST SP 800-161 also states, "organizations may be at risk to Information and Communications Technology (ICT) supply chain compromise through component service and repair processes. The organization should manage risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the ICT supply chain infrastructure."

USAID did not address the following SCRM processes in the *Supply Chain Risk Management Standard Operating Procedures*:

- Procedures to detect and prevent counterfeit components from entering the system.
- Requirements and procedures for reporting counterfeit system components.
- Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.

A recommendation was made in a December 2021 U.S. Government Accountability Office report[15] regarding USAID developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment. Therefore, we are not making a recommendation regarding counterfeit components.

Management stated that, although the *Supply Chain Risk Management Standard Operating Procedures* were finalized in July 2021, there are gaps in the procedures related to certain SCRM processes and they will continue to update the procedures.

Without fully addressing SCRM processes in USAID's procedures, certain SCRM processes may not be fully implemented. This may hinder USAID's ability to identify and mitigate supply chain risks. Therefore, we are making the following recommendation:

> ***Recommendation 2:*** *We recommend that USAID's Chief Information Officer address the management of system components requiring repair or service in its* Supply Chain Risk Management Standard Operating Procedures*.*

[15] Recommendation 145, "INFORMATION AND COMMUNICATIONS TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks " (GAO-171).

4. USAID NEEDS TO STRENGTHEN ITS INVENTORY MANAGEMENT PROCESS

Cybersecurity Framework Security Function: *Identify*
FY 2021FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control CM-8, Information System Component Inventory, states the following regarding inventory management:

> The organization:
> * * *
> d. Ensure the hardware inventory is at the level of granularity deemed necessary for tracking and reporting. The inventory specifications include:
> …
> 3) Physical location of hardware.

USAID ADS Chapter 545, Section 545.3.6.8, states:

> System Owners must:
> …
> d. Ensure the 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;
> 3. Physical location of hardware;
> 4. Software name, version number, and description; and
> 5. Software license information including number of licenses, etc. as applicable.

USAID did not document the physical location for 342 of 139,317 Information Technology (IT) assets in the hardware inventory, as required by USAID ADS Chapter 545. Management stated that the location was not captured in the inventory for all IT assets due to an oversight when the annual inventory update was performed.

Incomplete or inaccurate hardware inventories could result in a loss of confidentiality and waste. In addition, stolen or misplaced IT equipment could put USAID at a risk of loss of control of their 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.

Upon notification of this issue, management revised the inventory listing to include the location for all assets. Therefore, we are not making a recommendation at this time.

5. USAID Needs to Strengthen Mobile Device Management

Cybersecurity Framework Security Function: *Identify*
FY 2021 FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control AC-19, states the following regarding access control for mobile devices:

> The organization:
>
> a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

NIST SP 800-53, Revision 4*,* security control CM-7, states the following regarding unauthorized software/blacklist:

> Control Enhancement 4:
>
> * * *
>
> b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, states the following:

> General security recommendations for any IT technology are provided in NIST SP 800-53. Policy restrictions of particular interest for mobile device security include the following:
>
> - Limit or prevent access to enterprise services based on the mobile device's operating system version.
> - Restrict which applications may be installed through whitelisting (preferable) or blacklisting.

In the FY 2020 FISMA audit report,[16] we determined that USAID did not effectively implement controls over mobile devices issued and authorized for official use, including for application management. Specifically, we noted:

- USAID did not require mobile device users to install security and operating system updates within a prescribed period and deny access to its enterprise services for devices that were not updated within that prescribed period.
- USAID did not yet fully implement the ability to containerize mobile device software which would prevent the installation of unauthorized software.

Without technical controls preventing the installation of potentially harmful software on USAID mobile devices, employees may introduce dangerous software and malware into the USAID computing environment. Although USAID management took final corrective action on one of the prior recommendations[17] during this audit, they confirmed that they did not yet take final action on the other.[18] Therefore, CLA is not making a recommendation at this time.

[16] *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).

[17] Recommendation 5, *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).

[18] Recommendation 6, *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).

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft FISMA report, USAID agreed with the two recommendations. USAID's comments are included in their entirety in Appendix II.

USAID stated they completed final action and requested closure of recommendation 1 upon issuance of the final report. Based on our evaluation of the Agency's comments and review of the evidence provided, we agree that management implemented a process to automatically disable system user accounts after 90 days of inactivity for the sampled system tested. Therefore, we consider recommendation 1 closed.

USAID outlined its plans to address recommendation 2. We acknowledge management's decision on recommendation 2, and, therefore, consider recommendation 2 resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

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 audit was designed 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.

For this year's review, IG's were required to assess 66 metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The scope of this performance audit was to assess USAID's information security program consistent with FISMA and reporting instructions issued by OMB and DHS. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 6 of 52 internal and external information systems[19] in USAID's FISMA inventory as of February 12, 2021.

In addition, we performed an internal vulnerability assessment of USAID's Washington D.C. network. The audit also included a follow up on prior audit recommendations from the fiscal years 2018,[20] 2019,[21] and 2020[22] audit reports to determine whether USAID made progress in implementing them. See Appendix III for the status of the prior recommendations.

Audit fieldwork covered USAID's headquarters located in Washington, DC. In addition, the following overseas missions were included in two of our samples: Bangladesh, Ghana, Haiti, Kenya, Madagascar, Mozambique, Nicaragua, Nigeria, Republic of Guatemala, Rwanda, Senegal, Sri Lanka, South Africa, Thailand, and Uganda. Fieldwork was conducted from April 9, 2021, to September 2, 2021. It covered the period from October 1, 2020, through September 2, 2021.

[19] Ibid 6.

[20] Ibid 11.

[21] Ibid 12.

[22] Ibid 13.

Methodology

To determine if USAID implemented an effective information security program, we conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we 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, we compared documents, such as USAID's information technology policies and procedures, to requirements stipulated in NIST special publications. We also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, we reviewed the status of FISMA audit recommendations from fiscal years 2018, 2019, and 2020.[23]

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we 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, this resulted in selecting the entire population. However, in cases where 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, we followed a work plan based on, but not limited to, the following guidance:

- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements.*
- OMB and DHS, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- NIST Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[23] Ibid 11, 12, and 13.

Appendix II

MANAGEMENT COMMENTS

USAID
FROM THE AMERICAN PEOPLE

MEMORANDUM

TO: Deputy Assistant Inspector General for Audit, Alvin A. Brown

FROM: USAID, Sr. Deputy Chief Information Officer, Patrick Robinson /s/

DATE: November 08, 2021

SUBJECT: Management Comments to Respond to the Draft Audit Report Produced by the Office of Inspector General (OIG) titled, USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-000-22-00X-C) (AA150521)

The U.S. Agency for International Development (USAID) would like to thank the Office of the Inspector General (OIG) for the opportunity to provide comments on the subject draft report, *USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (A-000-22-00X-C) (AA150521). The Agency agrees with both recommendations, and herein provides plans for implementing them, and reports on significant progress already made.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE REPORT RELEASED BY THE OFFICE OF INSPECTOR GENERAL (OIG) TITLED, USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-000-22-00X-C) (AA150521)

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 2 recommendation(s) for USAID:

Recommendation 1: We recommend that USAID's Chief Information Officer implement a process to automatically disable system user accounts after 90 days of inactivity. If automatic disabling of accounts is not possible, we recommend the USAID's Chief Information Officer implement a daily review process to ensure that accounts are disabled after 90 days of inactivity.

- **Management Comments:** M/CIO agrees with the recommendation and believes that sufficient action has been taken to address it. Specifically, the system administrator for the identified system runs an internal batch job daily that automatically disables accounts that exceed 90 days of inactivity. Tab 1 of the attached spreadsheet (Tab B) shows the audit log of the "User Status Change Job" which is the batch job that runs at midnight every day to disable inactive accounts, for the months of July and August 2021. Tab 2 of the worksheet shows audit log instances of users deactivation events.

- **Target Completion Date:** M/CIO requests closure upon report issuance.

Recommendation 2: We recommend that USAID's Chief Information Officer address the management of system components requiring repair or service in its Supply Chain Risk Management Standard Operating Procedures.

- **Management Comments:** M/CIO agrees with the recommendation. We are currently in the process of maturing our Supply Chain Risk Management program, and will incorporate language into our Standard Operating Procedures to include the management of system components requiring repair or service.

- **Target Completion Date:** September 30, 2022

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 2018, FY 2019, and FY 2020[24] FISMA audit recommendations.

No.	FY 2018 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
1	We recommend that USAID's chief information officer update the Agency's Vulnerability Management Standard Operating Procedure to (1) define the timeframe for applying system patches and (2) document and implement a process to validate that system patches are applied according to the timeframe specified in the procedure.	Closed	Agree

No.	FY 2019 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
2	We recommend that USAID's chief information officer should update its hardware inventory policies to reflect the current operating environment.	Closed	Agree

No.	FY 2020 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
1	We recommend that USAID's Chief Information Officer should implement a process to document and implement mitigating controls for vulnerabilities that cannot be remediated in accordance with the timeframes defined by Agency policy.	Closed	Agree
2	We recommend 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 Agency policy.	Open	Agree, See Finding 1
3	We recommend USAID's Office of Human Capital and Talent Management should implement a process to maintain records electronically for onboarding and off-boarding staff.	Open	Agree, See Finding 1
4	We recommend USAID's Chief Information Officer should implement a process to validate that all privileged personnel receive the required specialized training prior to gaining system access.	Closed	Agree
5	We recommend USAID's Chief Information Officer update the mobile device policy to specify the time period users must apply security and operating system updates on Agency mobile devices and implement a process to deny access to	Closed	Agree

[24] Ibid 11, 12, and 13.

No.	FY 2020 Audit Recommendation	USAID Position on Status	Auditor's Position on Status
	Agency enterprise services for mobile devices that have not been updated within the prescribed period.		
6	We recommend USAID's Chief Information Officer develop and implement a process to block unauthorized applications from installing on Agency mobile devices.	Open	Agree, See Finding 5
7	We recommend USAID's Chief Information Officer should enhance the Agency's tracking process to include early warning indicators when testing of information system contingency plans will not be completed in the timeframes defined by USAID policy, and take corrective action.	Closed	Agree