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

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

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

Office of Inspector General, U.S. Agency for International Development

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: January 7, 2021

TO: USAID, Chief Information Officer, Jay Mahanand
USAID, Chief Human Capital Officer, Bob Leavitt

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

SUBJECT: USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA (A-000-21-004-C)

Enclosed is the final audit report on USAID's information security program for fiscal year 2020, 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 the 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 tested 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 auditors reviewed 6 of the 58 information systems in USAID's inventory as of April 17, 2020. Audit fieldwork covered USAID's headquarters located in

[1] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

Washington, DC, and included 12 overseas missions for certain tests. It was performed April 9, 2020, to September 28, 2020, and covered the period from October 1, 2019, to September 28, 2020.

CLA concluded that USAID generally implemented an effective information security program by implementing 123 of 135[2] instances of selected security controls for selected information systems. For example, USAID maintained an effective:

- Program for enterprise risk management.
- Incident handling and response program.
- Program for monitoring external service providers.
- Information systems backup program.

However, as summarized in the table below, CLA noted weaknesses in six of the eight FISMA metric domains.

Fiscal Year 2020 IG FISMA Metric Domains[3]	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	X
Information Security Continuous Monitoring	X
Incident Response	
Contingency Planning	X

To address the weaknesses identified in CLA's report, we recommend the following actions.

Recommendation 1. 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.

Recommendation 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 Agency policy.

[2] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. CLA tested 66 controls. A control was counted for each system it was tested against. Thus, there were 135 instances of testing a control.

[3] Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency's "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 17, 2020.

Recommendation 3. USAID's Chief Human Capital Officer should implement a process to maintain records electronically for onboarding and off boarding staff.

Recommendation 4. 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.

Recommendation 5. USAID's Chief Information Officer should 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 Agency enterprise services for mobile devices that have not been updated within the prescribed period.

Recommendation 6. USAID's Chief Information Officer should develop and implement a process to block unauthorized applications from installing on Agency mobile devices.

Recommendation 7. 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.

In addition, USAID has not taken final corrective action on one recommendation in our 2018 FISMA audit report and one recommendation in our 2019 FISMA audit report. See Appendix IV on pages 28-29 of CLA's report for the full text of the recommendations.

In finalizing the report, the audit firm evaluated USAID's responses to the recommendations. After reviewing that evaluation, we consider recommendation 1 open and unresolved; recommendations 2, 3, 5, and 6 resolved but open pending completion of planned activities; and recommendations 4 and 7 resolved but open pending OIG's verification of the agency's final actions.

We look forward to working with the agency to resolve recommendation 1. For recommendations 2, 3, 5, and 6, 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 2020

Final Report

CliftonLarsonAllen LLP
CLAconnect.com

December 11, 2020

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, D.C. 20005-2221

Dear Mr. Norman:

CliftonLarsonAllen LLP (CLA) is pleased to present our 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 2020.

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

Very truly yours,

S. M Mirzakhani

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

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 2020 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether USAID implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls for 6 of 58 of USAID's internal and external information systems. For this year's review, Inspectors General were also required to assess information security programs on a maturity scale from Level 1 (Ad Hoc) to Level 5 (Optimized) in eight IG FISMA Metric Domains and five Function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and the maturity level of each function area.

Audit fieldwork covered USAID's headquarters located in Washington, DC. In addition, the following overseas missions were included in two of our samples: Ethiopia, Liberia, Malawi, Morocco, Mozambique, Nepal, Nicaragua, Nigeria, Peru, Rwanda, Tanzania, and Thailand. Fieldwork was conducted from April 9, 2020 to September 28, 2020 and covered the period from October 1, 2019, through September 28, 2020.

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 generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. However, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in 6 of the 8 Inspector General FISMA Metric Domains and have made seven new recommendations to assist USAID in strengthening its information security program. In addition, we noted that two recommendations related to prior year FISMA audits were still 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 11, 2020. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to December 11, 2020.

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 USAID Office of Inspector General.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
December 11, 2020

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (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 USAID's information security program and practices. The objective of this performance audit was to determine whether USAID implemented an effective[2] information security program.

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) provide annual instructions to Federal agencies and IGs for preparing FISMA reports. On November 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year IGs are required to complete IG FISMA Reporting Metrics[3] to independently assess their agencies' information security programs.

[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 implementing certain security controls for selected information systems in support of FISMA.

[3] CLA submitted its responses to the FY 2020 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2020 IG FISMA Reporting Metrics are designed to assess the maturity[4] of the information security program and align with the 5 functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2020 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Metric Domains
Identify	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, CLA reviewed selected[5] controls related to the IG FISMA Reporting Metrics for 6 of 58 information systems[6] in USAID's FISMA inventory as of April 17, 2020.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

Audit Results

CLA concluded that USAID generally implemented an effective information security program by implementing 123 of 135[7] selected security control instances for selected information systems. For example, USAID maintained an effective:

- Program for enterprise risk management.
- Incident handling and response program.
- Program for monitoring external service providers.
- Information systems backup program.

[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.

[5] See Appendix III for a list of controls selected.

[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.

[7] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested 66 controls. A control was counted for each system it was tested against. Thus, there were 135 instances of testing a control. See Appendix III for a list of the controls.

Although USAID generally implemented an effective information security program, its implementation of 12 of the 135 control instances was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. As a result, CLA noted weaknesses in the following FISMA Metric Domains (Table 2) and made 7 recommendations to assist USAID in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2020 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Metric Domains	Weaknesses Noted in FY 2020
Identify	**Risk Management**	USAID Needs to Strengthen Mobile Device Management (**Finding 5**) USAID Needs to Strengthen Inventory Management (**Finding 6**)
Protect	**Configuration Management**	USAID Needs to Strengthen Vulnerability and Patch Management Controls (**Finding 1**)
	Identity and Access Management	USAID Needs to Strengthen Account Management Controls (**Finding 2**)
	Data Protection and Privacy	None
	Security Training	USAID Needs to Strengthen Security Training Requirements (**Finding 3**)
Detect	**Information Security Continuous Monitoring**	USAID Needs to Strengthen its Security Control Assessment Process (**Finding 4**)
Respond	**Incident Response**	None
Recover	**Contingency Planning**	USAID Needs to Strengthen Contingency Planning Controls (**Finding 7**)

In response to the draft FISMA report, USAID agreed with six of the seven recommendations. USAID disagreed with Recommendation 1, does not intend to take further action on it, and requested closure. USAID outlined its plans to address recommendations 2, 3, 5 and 6. USAID stated they completed final action and requested closure upon issuance of the final report for recommendations 4 and 7. Based on our evaluation of the Agency's comments, we do not agree with closure for recommendations 4 and 7 because there has not been sufficient time to determine if the corrective actions have been fully implemented. Therefore, we consider recommendations 4 and 7 open-resolved pending OIG's verification of the Agency's final actions. Furthermore, we acknowledge management's decisions on recommendations 2, 3, 4, 5, 6, and 7. 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, Appendix II includes USAID management comments, Appendix III identifies the controls selected for testing, and Appendix IV provides the status of prior year recommendations.

AUDIT FINDINGS

1. USAID Needs to Strengthen Vulnerability and Patch Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Configuration Management*

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security control System and Information Integrity (SI)-2, states the following regarding patch management:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [*Assignment: organization defined time-period*] of the release of the updates.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states:

> i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.
>
> Agencies shall:
> * * *
> 8. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement; and
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

Further, USAID's *Vulnerability Management and Remediation Standard Operating Procedure*, states that patches for critical vulnerabilities must be applied within 30 days. For vulnerabilities for which patches are not available, a risk acceptance must be documented until a permanent solution is available and compensating security controls, (also known as mitigating controls) are required in order to mitigate the vulnerability.

USAID's internal monthly vulnerability scans[8] identified critical[9] security vulnerabilities related to patch management and unsupported software. Although some vulnerabilities were within the allowable timeframe for them to be remediated, critical vulnerabilities related to Windows 7, Oracle Java, Office 365, and Adobe accounting for 79% of the critical vulnerabilities were past the required remediation timeframe. These vulnerabilities were published by the applicable vendor from 1999 to February 2020. Management

[8] USAID performed the vulnerability scans during FY 2020.

[9] Nessus applies a Critical severity to any vulnerability having a Common Vulnerability Scoring System (CVSS) Base score of 10 on a scale of 1-10. Critical vulnerabilities could allow remote code execution without user interaction or where code executes without warnings or prompts.

indicated they were aware of the vulnerabilities and taking steps to remediate them. However, USAID encountered challenges in obtaining an updated software license needed to remediate the identified vulnerabilities and in updating unsupported software on devices due to remote operations during a pandemic. In addition, management stated risk acceptances are documented in the Plan of Action and Milestones (POA&Ms) for the vulnerabilities' until such time they are addressed; however CLA determined that mitigating controls were not documented for the vulnerabilities as required in the USAID's *Vulnerability Management and Remediation Standard Operating Procedure*. CLA made a recommendation in the FY 2018 FISMA audit report[10] regarding patching and remediating vulnerabilities in a timely manner. Because identified vulnerabilities have continued to exceed the allocated timeframe for remediation, CLA considers this recommendation still open and is not making a new recommendation.

Additionally, CLA made a recommendation in the FY 2018 FISMA audit report[11] regarding acceptance of risk for allowing unsupported software. Management accepted the risk for allowing unsupported software. Therefore, CLA determined that USAID took corrective action on the recommendation. However, as previously stated, USAID has not executed a process for implementing mitigating security controls for vulnerabilities that are not able to be remediated in accordance with the timeframes defined by USAID policy.

Without implementing mitigating controls, the confidentiality, integrity, and availability of information is at risk. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Authorized USAID employees may be unable to access systems.
- USAID data may be lost, stolen, or compromised.

CLA is making the following recommendation to address the identification, documentation, and implementation of mitigating controls:

> ***Recommendation 1:*** *USAID 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 USAID policy.*

2. USAID Needs to Strengthen Account Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 4, security controls related to temporary accounts, access agreements, personnel termination, and account management, state the following:

> AC-2 – Account Management
> The Organization:
> ***

[10] Recommendation 1, *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).
[11] Recommendation 2, *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts.

Control Enhancements:

***

2) The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time-period for each type of account]

PS-4 – Personnel Termination

The Organization:

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

PS-6 – 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.

USAID ADS Chapter 545, Section 545.3.2.2*, Information Systems Security*, states the following regarding temporary accounts:

> If emergency and temporary accounts are authorized, the system must be configured to automatically disable the accounts after 30 days. Accounts for users on extended absences must be temporarily suspended or disabled and the System Owner (SO) must establish a process to re-enable such accounts.

In addition, the security plan for one system states the following regarding access agreements and personnel termination:

> Approvals by system Information System Security Officer (ISSOs) and System Owner (SOs) designees are required for requests to create information system accounts and authorize access to the information system based on:
>
> a. A valid access authorization
>
> Disables information system access within two weeks of transfer or termination.

Furthermore, the USAID *AID Form 451-1, Employee Exit Clearance for Separation or Moving Within USAID,* states "All USAID employees separating from the Agency or moving to another USAID office, bureau or mission must complete applicable sections of Form AID 451-1 and obtain the requested clearances."

USAID did not effectively manage user accounts for 1 of 6 sampled systems. Specifically, for one system, the following was identified:

- Four of 12 identified temporary accounts were not disabled after 30 days as required by USAID policy due to an oversight by staff. Upon notification of the issue to management, the accounts were disabled. Therefore, we are not making a recommendation.

- Accounts for 13 from a total population of 226 separated employees were not disabled. Management stated that although the employees are listed as separated on the report provided, the individuals are still active employees. Office of Human Capital and Talent Management (HCTM) and Office of Acquisition and Assistance (OAA) did not provide evidence to validate their employment status.

  In addition, we tested whether accounts for 23 separated employees were disabled within two weeks of their separation date in accordance with USAID policy. We found that 8 employee's accounts were not disabled timely in accordance with the policy. Management stated that 4 of the 8 are still active employees, however HCTM and OAA did not provide evidence to validate their employment status. Management agreed that the remaining 4 accounts were not disabled timely in accordance with policy. Management acknowledged there was not a process in place to verify that separated employee's accounts were disabled timely in accordance with USAID policy.

- Exit checklists were not provided for 11 of 23 sampled separated individuals. Therefore, we were not able to validate whether USAID's information technology assets were returned and accounted for. Management stated that HCTM and OAA were not able to locate the exit forms.

- From a sample of 25 new hires from the total population of 266 new hires, evidence was not provided for 4 users to validate their access was approved and access agreements were signed prior to system access. According to USAID management, many of the documents could not be provided because they are available only in hard copies, not electronically, and some offices were closed due to a pandemic.

Without ensuring accounts are disabled due to inactivity, temporary status, position change, 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 access to inappropriate 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. Therefore, CLA is making the following recommendations:

Recommendation 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.*

Recommendation 3: *USAID's Chief Human Capitol Officer should implement a process to maintain records electronically for onboarding and off boarding staff.*

3. USAID Needs to Strengthen Security Training Requirements

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Security Training*

NIST SP 800-53, Revision 4, security controls regarding security training and role-based training, state the following:

> AT-2 – Security Awareness and Training Policy and Procedures
> The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
>
> a. As part of initial training for new users.
>
> AT-3 – Role-based Security Training
> The organization provides role-based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties.

The USAID ADS Chapter 545, security control AT-2 and AT-3, states the following regarding security awareness training and role-based training:

> AT-2 – Security Awareness Training
> Initial Security and Privacy Awareness Training: All USAID staff or others working on behalf of USAID accessing USAID systems must receive initial training in security awareness and accepted security practices. Staff must complete security awareness training prior to being granted a user account. When access to an Information System is required by contract, the Contracting Officer's Representative (COR) must ensure that contractors complete the necessary training sessions.
>
> AT-3 – Role-based Security Training
> All USAID staff and others working on behalf of USAID with significant security responsibilities (i.e., ISSOs and SAs) must receive role-based training specific to their security responsibilities upon assignment to the role, and refresher training yearly thereafter.

Evidence was not provided to validate the completion of initial security awareness training for 4 out of 25 sampled new hires. As discussed in Finding 2, management stated electronic evidence of training was not maintained. The users are located at missions and the training records were not available due to mission closure during the pandemic.

Additionally, 2 out of 3 sampled users from a population of 26 new privileged users did not complete specialized training prior to gaining access to one system. Management stated there was not a process to validate that all privileged personnel received the required specialized training prior to gaining system access.

Without maintaining records and ensuring individuals complete their required training for access, there is increased risk that system users do not fully understand their responsibilities when accessing USAID information systems and managing agency data. In addition to recommendation 3, we are making the following recommendation.

> ***Recommendation 4:*** *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.*

4. USAID Needs to Strengthen its Security Control Assessment Process

Cybersecurity Framework Security Function: *Detect*
FY 2020 FISMA IG Metric Domain: *Information Security Continuous Monitoring*

USAID ADS Chapter 545*,* states the following regarding Security Assessments:

> CA-2 – Security Assessments
> SOs must assess the security controls in their information systems and their environment of operation at least annually to determine the extent to which the controls are:
> a. Implemented correctly,
> b. Operating as intended, and
> c. Producing the desired outcome with respect to meeting established security requirements.
>
> RA-3 – Risk Assessment
>
> c. Update the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

NIST SP 800-53, Revision 4, requires organizations to conduct an assessment of risk,[12] including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

For two systems, USAID did not conduct security control assessments annually in accordance with USAID policy. Specifically, security control assessments for one system were conducted in 2017 and 2020, but not in 2018 and 2019. For the other system, assessments were conducted in 2018 and 2020, but not in 2019. Additionally, risk assessments for three systems were not updated annually as required by USAID policy.

[12] NIST and OMB define risk as: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."

USAID procedures regarding the escalation process for non-compliance with continuous monitoring requirements were not fully developed and disseminated until July 15, 2019. Therefore, at the time the assessments were not completed in prior years, there was not a formal process for addressing non-compliance with the security control assessment annual requirements.

Without conducting annual security control assessments, USAID is at risk of being unaware of the current weaknesses and risks to its information system environment. Since the control assessments were completed in 2020 and USAID's escalation process for non-compliance with continuous monitoring requirements has been implemented, CLA is not making a recommendation at this time.

5. USAID Needs to Strengthen Mobile Device Management

Cybersecurity Framework Security Function: *Identify*
FY 2020 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.

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 USAID enterprise services for devices that were not updated within that prescribed period. Management

stated that USAID has a manual process to deny access to USAID enterprise services when security and operating system updates are not applied to mobile devices. The process utilizes an enterprise mobility management software to discover devices out of compliance and a direct email communication with the end user and manager. After a period of time, USAID email will be removed from the device. However, USAID did not provide evidence that is process was in place.

- USAID did not implement a process to prevent users from installing/downloading unauthorized software on their official mobile devices. Management stated that USAID has not yet fully implemented the ability to containerize mobile device software which would prevent the installation of unauthorized software. This will be implemented in 2021.

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. In addition, without specifying how quickly users must apply available security and operating system updates, and without an automated tool to validate and enforce compliance, USAID allows its mobile devices to remain vulnerable to potential security threats. Therefore, CLA is making the following recommendations:

Recommendation 5: *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 Agency enterprise services for mobile devices that have not been updated within the prescribed period.*

Recommendation 6: *USAID's Chief Information Officer develop and implement a process to block unauthorized applications from installing on Agency mobile devices.*

6. USAID Needs to Strengthen its Inventory Management

Cybersecurity Framework Security Function: *Identify*
FY 2020 FISMA IG Metric Domain: *Risk Management*

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/manufacture name and component name;
> 2. Hardware model number, item description, and serial number;
> 3. Hardware configuration;
> 4. Software version number and description;
> 5. Software license information including seats, number of licenses, etc. as applicable; and
> 6. Physical location of hardware.

USAID did not include the following fields in the hardware inventory as required by USAID ADS Chapter 545, Section 545.3.6.8:

- Hardware Configuration
- Software Version Number and Description

Management stated the requirements in ADS Chapter 545 were outdated and no longer reflective of the information that management intends to collect and is currently collecting. Without a proper hardware inventory listing, incomplete or inaccurate inventories could result in a loss of confidentiality and waste. Stolen or misplaced computing 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 USAID budget as unplanned and unnecessary spending may be required to replace stolen or misplaced computing equipment.

A recommendation addressing this finding was made in the fiscal year 2019 FISMA audit.[13] Management stated that the inventory management issues are still being addressed. Since the recommendation remains open, we are not making a new recommendation.

7. USAID Needs to Strengthen Contingency Planning Controls

Cybersecurity Framework Security Function: *Recover*
FY 2020 FISMA IG Metric Domain: *Contingency Planning*

NIST Special Publication 800-53, Revision 4, security control CP-4, states the following regarding Contingency Plan Testing:

> The organization:
> a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
> b. Reviews the contingency plan test results; and
> c. Initiates corrective actions, if needed.

ADS Chapter 545, section 545.3.7.3, security control CP-4, states that "SOs must test CPs for their information system(s) annually."

Information system contingency plan testing was not conducted annually for one system as required by USAID policy. The contingency plan was tested in 2018 and 2020, but not in 2019. USAID has a process in place to track contingency plan testing; however, due to management oversight contingency plan testing was not conducted in 2019 for that system.

Without completing contingency plan testing of the system, USAID may be unprepared for system recovery should the Agency's information systems be disrupted or otherwise unavailable. Therefore, CLA is making the following recommendation.

[13] Recommendation 2, *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).

Recommendation 7: *USAID's Chief Information Officer should enhance the 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.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft FISMA report, USAID agreed with six of the seven recommendations. USAID disagreed with Recommendation 1, does not intend to take further action on it, and requested closure. USAID reached a decision and outlined is plans to address recommendations 2, 3, 5 and 6. USAID stated they completed final action and requested closure upon issuance of the final report for recommendations 4 and 7. Based on our evaluation of the Agency's comments, we do not agree with closure for recommendations 4 and 7 because there has not been sufficient time to determine if the corrective actions have been fully implemented. Therefore, we consider recommendations 4 and 7 open-resolved pending OIG's verification of the Agency's final actions. Furthermore, we acknowledge management's decisions on recommendations 2, 3, 4, 5, 6, and 7. USAID's comments are included in their entirety in Appendix II. The following paragraphs describe our evaluation of management comments in detail.

USAID disagreed with Recommendation 1 pertaining to vulnerability and patch management. USAID stated that sufficient processes had already been implemented to address mitigating controls for vulnerabilities that cannot be remediated in accordance with Agency defined policy and requested closure upon issuance of the final report. USAID stated these processes include temporarily accepting risk via the POA&M process until a permanent solution is safely implemented, and requiring compensating security controls in order to mitigate the vulnerability. However, as stated in the report, we determined that compensating controls were not documented for the vulnerabilities that were not remediated in accordance with Agency defined policy, and evidence was not provided to validate that USAID implemented any compensating controls in order to reduce the risk to the Agency's network and data. If USAID had documented and implemented compensating controls to directly mitigate the vulnerabilities in their risk acceptance process, risk related to the vulnerabilities would likely be reduced. We strongly urge USAID to revise its response to address this issue and we do not agree recommendation 1 should be closed. Therefore, we consider recommendation 1 open-unresolved.

USAID agreed with recommendations 2 and 3 but requested that the OIG update the recommendations to include additional USAID Bureaus and Independent Offices that will be necessary to address the weaknesses. While we did not revise the recommendations, in subsequent correspondence, USAID indicated that their responses are their management decisions. Therefore, we consider recommendations 2 and 3 open-resolved.

For recommendation 4, we agree that a process has been developed to validate that new privileged users have completed role-based training. However, there has not been sufficient time to determine if management has implemented that process to confirm that role-based training is completed prior to granting privileged access. Therefore, we consider recommendation 4 open-resolved pending OIG's verification of the Agency's final actions.

For recommendations 5 and 6, USAID provided its proposed corrective action plans and target completion dates to address the weaknesses. Therefore, we consider recommendations 5 and 6 open-resolved pending completion of planned activities.

For recommendation 7, we agree that the Office of the Chief Information Officer maintains a dashboard of all disaster recovery tests conducted. However, there has not been sufficient time to determine if management has implemented the monitoring process described for validation and follow-up actions by senior leadership. Therefore, we consider recommendation 7 open-resolved pending OIG's verification of the Agency's final actions.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with GAGAS. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the 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[14] information security program.

The audit included tests of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed USAID's performance and compliance with FISMA in the following areas:

- Access Controls
- Accountability, Audit, and Risk Management
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Service Acquisition

For this audit, CLA reviewed selected controls related to the FY 2020 IG FISMA Reporting Metrics from 6 of 58 information systems in USAID's systems inventory as of April 17, 2020. See Appendix III for a listing of the controls selected.

The audit also included a follow up on prior audit recommendations for FY 2018[15] and FY 2019[16] to determine if USAID made progress in implementing the recommended improvements concerning its information security program. See Appendix IV for the status of prior year recommendations.

[14] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

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

[16] *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).

Audit fieldwork covered USAID's headquarters located in Washington, DC. In addition, the following overseas missions were included in two of our samples: Ethiopia, Liberia, Malawi, Morocco, Mozambique, Nepal, Nicaragua, Nigeria, Peru, Rwanda, Tanzania, and Thailand. Fieldwork was conducted from April 9, 2020 to September 28, 2020 and covered the period from October 1, 2019, through September 28, 2020.

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 NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. Further, CLA reviewed the status of FISMA audit recommendations from fiscal year 2018 and 2019.[17]

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. 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 used the following guidance:

- OMB and DHS, *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular Number A-130, *Managing Information as a Strategic Resource.*
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[17] Ibid., footnotes 15 and 16.

MANAGEMENT COMMENTS

The following represents the full text of USAID's management comments on the draft report.

USAID
FROM THE AMERICAN PEOPLE

MEMORANDUM

TO: Alvin Brown, Deputy Assistant Inspector General (A/AIG)

FROM: Jay Mahanand, Chief Information Officer (CIO) /s/

DATE: December 4, 2020

SUBJECT: Management Comments to Respond to the Draft Report Produced by the Office of the U.S. Agency for International Development (USAID) Inspector General (OIG) titled, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of [the Federal Information Security Management Act, FISMA]* (A-000-21-00X-C).

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 Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (A-000-21-00X-C). The Agency agrees with six out of the seven recommendations, and herein provides plans for implementing them, and reports on significant progress already made. For the one recommendation with which we disagree, we outline our existing documentation and procedures that we believe fully address it.

Tab A—Management Decisions

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON THE DRAFT REPORT RELEASED BY THE OFFICE OF THE INSPECTOR GENERAL TITLED, *USAID HAS GENERALLY IMPLEMENTED CONTROLS IN SUPPORT OF [THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT, FISMA] FOR FISCAL YEAR 2020* (A-000-21-00X-C)

Please find below the Management Decisions and corrective actions from the U.S. Agency for International Development (USAID) on draft report A-000-21-00X-C produced by the Office of the USAID Inspector General (OIG), which contains seven recommendations for the Agency:

Recommendation 1: USAID's Chief Information Officer (CIO) 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.

- **Management Decision:** USAID disagrees with this recommendation. We insist the Agency is complying fully with the dispositive Federal standards for managing information-technology (IT) vulnerabilities as defined by the National Institute for Standards and Technology (NIST) within the U.S. Department of Commerce (DOC) in Revision 2 of Special Publication 800-37, "Risk Management Framework For Information Systems And Organizations - A System Life-Cycle Approach for Security and Privacy (RMF)."

  Specifically, DOC/NIST indicates that using the RMF rigorously provides senior leaders and executives of Federal Departments and Agencies with the necessary information to make efficient, cost-effective, risk-management decisions about the IT systems that support their missions and business functions. Page 72 of the RMF, in the section titled, "Risk Response," states the following:

  > "*After risk is analyzed and determined, organizations can respond to risk in a variety of ways, including acceptance of risk and mitigation of risk*."

  DOC/NIST is clear that Departments and Agencies can accept and mitigate IT risks, and does not demand 100-percent elimination of them. Acceptable responses according to Revision 2 of Special Publication 800-37 can include using Plans of Action and Milestones (POA&Ms), amending Standard Operating Procedures (SOPs) for managing vulnerabilities to consider alternative courses of actions, and weekly briefings to senior leadership. USAID asserts that we have in place, and are implementing and documenting, sufficient controls, risk analyses, and response processes to mitigate any IT vulnerabilities that we cannot immediately remediate in accordance with our policies.

  POA&Ms - As part of the audit process, USAID provided the OIG with evidence of POA&Ms for all our IT vulnerabilities that exceeded their established remediation time. These POA&Ms serve as the Agency's documentation that we accept the risk of continuing to operate IT systems with known vulnerabilities, until we can remediate them completely or remove the device(s) from our network. Our policies and procedures comply with the RMF's guidance, and provide sufficient information for our CIO to make risk-based decisions consistent with the approach to Enterprise Risk-Management reflected in our Agency Risk Profile.

  SOPs for Managing Vulnerabilities - In September 2019, USAID amended our SOPs for Vulnerability-Management (Tab B) in September 2019 specifically to address this issue later raised in by the OIG in draft report A-000-21-00X-C. Section 1.1 of the SOPs, *Outcomes,* states that one of the targeted outcomes of vulnerability-management

includes "maintain[ing] IT systems against USAID-defined severity-remediation deadlines to patch, test and implement patches across the enterprise to reduce, remove, or receive risk-acceptance by the development of [POA&Ms] for all vulnerabilities that exceed the initial severity-remediation deadlines." Further, Section 3.3 of the SOPs. *Vulnerability Categorization, Triage, Tracking, and Change Controls,* states the following:

"In situations where it is determined that a security patch or vulnerability-remediation configuration change may result in the loss of functionality, performance, or availability, alternate courses of action may be used. The Security Operations, Information Technology Operations (ITO), and Information Assurance (IA) Management teams [in the Office of the CIO in the Bureau for Management] will work with the System Owners by providing recommendations for alternatives. These recommendations may include one or more of the following:

- Accept the risk of system impact and apply the patches or configuration changes;
- Removal of the affected devices, software, or configuration,
- Shut down or otherwise isolate the affected system(s) to eliminate the vulnerability;
- Temporary risk-acceptance via the POA&M process until a permanent solution is safely implemented;
- Require compensating security controls, alternative configuration changes or a workaround in order to mitigate the vulnerability; and accept the residual risk;
- Transfer the risk of exploitation to a third party (when possible); and
- Long-term risk-acceptance via the USAID Authorizing Official."

Weekly briefings with the CIO and Senior Leadership - Finally, the Office of the CIO in the Bureau for Management (M) conducts briefings on a weekly basis with the CIO and other senior leaders to review the status of unmitigated vulnerabilities and all open or overdue POA&Ms. M/CIO has developed dashboards (Tab C) to track these weaknesses, and uses these briefings as a mechanism to raise awareness and distribute resources to ensure the Agency takes appropriate actions to remediate any critical vulnerabilities as soon as possible.

- **Target Date:** We would welcome the chance to continue to discuss whether a recommendation might be necessary in this area. Because we have the aforementioned procedures in place and use them appropriately according to standards set by DOC/NIST, USAID does not agree that any further actions are required to address the recommendation as written. Therefore, we request closure of the recommendation upon the OIG's issuance of a Final Report.

Recommendation 2: USAID's CIO should collaborate with the Office of Human Capital and Talent Management (HCTM) to document and implement a process to verify that separated employees' accounts are disabled in a timely manner in accordance with Agency policy.

- **Management Decision:** USAID agrees completely that we should be able to disable the IT accounts of separated employees as soon as possible, and verify we have done so. However, we request that the OIG re-write this recommendation to address the root cause of the finding and make it more actionable for the Agency. A collaborative effort between several of USAID's Bureaus and Independent Offices will be necessary to solve the challenge. Therefore, the Agency requests that the OIG includes the Office of Acquisition and Assistance (OAA) in the M Bureau in the recommendation to ensure we can incorporate all of the Agency's hiring mechanisms and employee categories. HCTM provided the OIG with reports of U.S. Direct-Hire (USDH) employees and U.S. Personal Service Contractors (PSC) who have separated from the Agency. However, the reports do not accurately reflect that USDH and USPSCs do move between different hiring categories and contract mechanisms and therefore do not separate from the Agency. M/CIO will collaborate with HCTM and M/OAA to document and implement collectively a process by which we can better identify these situations and properly reconcile and validate separation reports. Pending an updated recommendation, M/CIO will work with HCTM and M/OAA to provide a Management Decision within the six-month period allowed.

- **Target Completion Date:** November 30, 2021.

Recommendation 3: USAID's Chief Human Capital Officer should implement a process to maintain records electronically for onboarding and offboarding staff.

- **Management Decision:** The Agency requests that the OIG re-write this recommendation to address the root cause of the finding and make it more actionable for the Agency. Specifically, the Agency requests that the recommendation include M/OAA and the Office of Management Services (MS) in the M Bureau to ensure we can incorporate the Agency's multiple hiring mechanisms and employee categories. Given that responsibility for the policy and management of the Agency's various employee categories falls to different Bureaus and Offices, maintaining electronic records of onboarding and offboarding staff requires collaboration between M/CIO, HCTM, M/OAA, and M/MS to ensure an enterprise-wide solution that captures all USAID personnel. Pending an updated recommendation, M/CIO and HCTM will work with M/OAA and M/MS to provide a Management Decision within the six-month period allowed.

- **Target Completion Date:** November 30, 2021.

Recommendation 4: USAID's CIO should implement a process to validate that all privileged personnel receive the required specialized training prior to gaining system access.

- **Management Decision:** USAID agrees with the recommendation, and we believe we have taken sufficient actions to close it. Specifically, M/CIO developed and

implemented role-based training for administrators (Tab D), which captures the requirements associated with having elevated privileges to USAID's systems. In addition, at the end of the training, users must acknowledge the roles, responsibilities, and best practices discussed throughout the presentation (Tab E). Further, to ensure users complete this training prior to receiving a privileged account, USAID has implemented an automated process through ServiceNow that requires that administrators who create a new privileged account also validate that the future account user has taken the specialized security training prior to completing the ServiceNow ticket and creating the account. This validation takes place by reviewing the master tracker of all users who have completed the specialized training (Tab F).

- **Target Date:** USAID requests closure of the recommendation upon the OIG's issuance of a Final Report.

Recommendation 5: USAID's CIO should 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 Agency enterprise services for mobile devices that have not been updated within the prescribed period.

- **Management Decision:** USAID agrees with the recommendation. M/CIO is in the process of implementing a procedure that will give users 30 days after a new operating system is released to update their mobile devices. Failure to do so will result in the disablement of the account, which will block the user from all USAID IT resources. In addition, M/CIO intends to issue an Agency Notice by the end of Calendar Year 2020, and another one in early 2021, to inform USAID's staff that we will be enforcing our policy to block non-compliant devices.

- **Target Date:** March 31, 2021.

Recommendation 6: USAID's CIO should develop and implement a process to block unauthorized applications from installing on Agency mobile devices.

- **Management Decision:** USAID agrees with the recommendation. The functionality needed to accomplish the goal of blocking applications requires the Agency to activate Apple Device Supervision on all Government-furnished mobile devices. Unfortunately, this functionality is not active on 4,700 of USAID's older devices. M/CIO is currently wiping and refreshing these devices on a rolling basis to apply the necessary mobile-device management settings.

- **Target Date:** September 30, 2021.

Recommendation 7: USAID's CIO 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.

- **Management Decision:** USAID agrees with the recommendation, and believes we have taken sufficient action to close it. Specifically, prior to the Agency's migration to the Azure cloud in 2019, M/CIO tested many system contingency plans on an individual basis, and the tracking of these tests was not always effective. Since the migration, in Fiscal Year (FY) 2020 M/CIO has refined and matured the process for testing the Agency's disaster-recovery and contingency processes on a quarterly basis, which exceeds the requirement for an annual test, and ensures the inclusion of the Agency's applications in these tests. M/CIO maintains a dashboard of all disaster-recovery tests conducted, which includes the scenario and success or failure of the test for each application (Tab G). M/CIO's senior leadership reviews these dashboards periodically for validation and follow-up actions as necessary. Based on the matured frequency and tracking of these contingency tests, M/CIO does not believe including early-warning indicators are a necessary action item, as the current process has made that matter irrelevant.

- **Target Date:** USAID requests closure of the recommendation upon the OIG's issuance of a Final Report.

SUMMARY OF CONTROLS TESTED

Control	Control Name	No. of Control Instances Tested
AC-1	Access Control Policy and Procedures	1
AC-17	Remote Access	1
AC-2	Account Management	6
AC-8	System Use Notification	1
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	6
AR-4	Privacy Monitoring and Auditing	1
AR-5	Privacy Awareness and Training	1
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-Based Security Training	2
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	3
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	3
CA-6	Security Authorization	6
CA-7	Continuous Monitoring	3
CM-1	Configuration Management Policy and Procedures	1
CM-10	Software Usage Restrictions	1
CM-2	Baseline Configuration	2
CM-3	Configuration Change Control	2
CM-6	Configuration Settings	3
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	3
CM-9	Configuration Management Plan	3
CP-1	Contingency Planning Policy and Procedures	1

Control	Control Name	No. of Control Instances Tested
CP-2	Contingency Plan	3
CP-3	Contingency Training	3
CP-4	Contingency Plan Testing	3
CP-6	Alternate Storage Site	3
CP-7	Alternate Processing Site	3
CP-8	Telecommunications Services	3
CP-9	Information System Backup	3
IA-1	Identification and Authentication Policy and Procedures	1
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
IR-7	Incident Response Assistance	1
MP-3	Media Marking	1
MP-6	Media Sanitization	1
PL-2	System Security Plan	3
PL-4	Rules of Behavior	3
PL-8	Information Security Architecture	3
PM-11	Mission/Business Process Definition	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	3
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	6
SA-3	System Development Life Cycle	3
SA-4	Acquisition Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	3

Control	Control Name	No. of Control Instances Tested
SC-28	Protection of Information at Rest	3
SC-8	Transmission Confidentiality and Integrity	3
SE-2	Privacy Incident Response	1
SI-2	Flaw Remediation	3
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	2
SI-7	Software, Firmware, and Information Integrity	2
	Total Control Instances Tested	**135**

STATUS OF PRIOR RECOMMENDATIONS

The following table provides the status of the FY 2018 FISMA audit recommendations.[18]

FY 2018 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	Disagree, see finding 1.
2. We recommend that USAID's Chief Information Officer document and implement a process to validate that unsupported software is either upgraded or removed within 48 hours of identification, as specified in the Agency's Unauthorized/Unsupported Software Standard Operating Procedures, or document acceptance of the risk for allowing the unsupported software on the network.	Closed	Agree
5. We recommend that USAID's Chief Information Officer document and implement a process to validate that USAID procedures are followed for testing, conducting security impact analysis of, and approving system changes.	Closed	Agree

The following table provides the status of the FY 2019 FISMA audit recommendations.[19]

FY 2019 Recommendation	USAID Position on Status	Auditor's Position on Status
1. USAID's Chief Information Officer document and implement a process to confirm that approval of user access is documented prior to granting access to the system for which verbal approvals had been allowed.	Closed	Agree
2. USAID's Chief Information Officer should update its hardware inventory policies to reflect the current operating environment.	Open	Agree
3. USAID's Senior Agency Official for Privacy should document and implement a process to	Closed	Agree

[18] Ibid., footnote 15.
[19] Ibid., footnote 16.

FY 2019 Recommendation	USAID Position on Status	Auditor's Position on Status
continuously monitor and review privacy controls in accordance with the Privacy Continuous Monitoring Strategy.		
5. USAID's Chief Information Officer should document backup procedures for the current operating environment.	Closed	Agree
6. USAID's Chief Information Officer should update acquisition policies and procedures to include security requirements outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, control SA 4 – Acquisition Process, for all information technology acquisitions.	Closed	Agree