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

FISMA: USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Longstanding Weaknesses Persist

Audit Report A-000-24-005-C
September 19, 2024

Office of Audits, Inspections, and Evaluations

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

MEMORANDUM

DATE: September 19, 2024

TO: Jason Gray
Chief Information Officer
USAID

Sepideh Keyvanshad
Acting Chief Human Capital Officer
USAID/Office of Human Capital and Talent Management

FROM: Paul K. Martin
Inspector General PaKMA

SUBJECT: FISMA: USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Longstanding Weaknesses Persist (A-000-24-005-C)

Enclosed is the final audit report on USAID's information security program for fiscal year (FY) 2024, in support of the Federal Information Security Modernization Act of 2014 (FISMA).[1] The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates LLC (RMA) to conduct the audit. The contract required RMA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed RMA'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. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which RMA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USAID implemented an effective information security program.[2] To answer the audit objective, RMA assessed the effectiveness of USAID's

[1] Pursuant to the Pub. L. No. 117-263 § 5274, USAID OIG provides nongovernmental organizations and/or businesses specifically identified in this report 30 days from the date of report publication to submit a written response to USAID OIG. Any comments received will be posted on https://oig.usaid.gov/. Please direct inquiries to oignotice_ndaa5274@usaid.gov.
[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year IG FISMA reporting metrics.

implementation of the FY 2024 IG FISMA reporting metrics[3] that fall into the nine domains in the following table. Also, RMA assessed USAID's implementation of applicable controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations," updated December 2020.

RMA reviewed 6 judgmentally selected systems of the 72 in USAID's inventory as of October 16, 2023. The audit team conducted its work from September 15, 2023, to June 26, 2024, for the period from October 1, 2023, through June 26, 2024. Fieldwork covered USAID's headquarters in Washington, DC, and included eight overseas missions for certain tests.

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

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured that the hardware and software assets connected to the network were covered by an organization-wide hardware/software asset management capability and were subject to the monitoring processes defined within the organization's Information System Continuous Monitoring Strategy.
- Employed automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to USAID's network.
- Measured the effectiveness of its awareness program and monitored qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices.
- Employed automated mechanisms to test system contingency plans more thoroughly and effectively.

However, as summarized in the table below, RMA found weaknesses in four of nine IG FISMA metric domains.[4]

Fiscal Year 2024 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	
Supply Chain Risk Management	X

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

[4] We also identified control weaknesses related to identity and access management and information security continuous monitoring in our recent audit report on USAID's use of cloud computing services. See USAID OIG, *Cloud Computing: USAID Needs to Improve Controls to Better Protect Agency Data* (A-000-24-004-P), September 16, 2024.

Fiscal Year 2024 **IG FISMA Metric Domains**	**Weaknesses** **Identified**
Configuration Management	
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	X
Incident Response	X
Contingency Planning	

RMA also determined that USAID did not take final action on two prior recommendations to correct longstanding weaknesses identified in our FY 2020 FISMA audit report.[5] According to Agency officials, the offices responsible for implementing the recommendations only managed a portion of the processes in which the weaknesses occurred, but actions were needed from multiple business units to complete final action. This lack of cooperation has led to challenges for the Agency in closing the recommendations. Refer to Appendix II of RMA's report for the status of prior year recommendations.

We are making seven recommendations, of which two are related to prior FISMA audit recommendations that USAID has not yet implemented. To address the weaknesses identified in the report, we recommend the following:

Recommendation 1. We recommend that USAID's Chief Information Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not timely disabling network accounts for separated employees and contractors, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 2.

Recommendation 2. We recommend that USAID's Chief Human Capital Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not maintaining records evidencing that staff have been off-boarded in accordance with Agency policy, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 3.

Recommendation 3. We recommend that USAID's Chief Information Officer develop and implement procedures to document deviations from Agency policy on security control assessments, including acceptance of the risk of such deviations.

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

Recommendation 4. We recommend that USAID's Chief Information Officer implement accurate automated dashboards to provide enterprise-wide metrics to inform top management of its information technology risks.

Recommendation 5. We recommend that USAID's Chief Information Officer establish and implement a process to track the progress of conducting annual reviews and related lessons learned from the implementation of its Information Security Continuous Monitoring Strategy.

Recommendation 6. We recommend that USAID's Chief Information Officer establish a formal training program in counterfeit component detection to educate responsible personnel. The training should cover identifying counterfeit hardware, software, and firmware components and should be updated regularly.

Recommendation 7. We recommend that USAID's Chief Information Officer update the event logging checklist to include details of event logging level 3 (advanced) applicability and implement requirements as specified by Office of Management and Budget Memorandum M-21-31.

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

RMA Associates

Auditors. Consultants. Advisors.

United States Agency for International Development (USAID)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2024

RMA | Associates
Auditors. Consultants. Advisors.

September 13, 2024

Inspector General
United States Agency for International Development
Washington, D.C.

RMA Associates, LLC, an independent certified public accounting firm, conducted a performance audit of the United States Agency for International Development's (USAID) compliance 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 scope of this audit was to assess USAID's information security program, which is consistent with FISMA, and reporting instructions issued by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. The audit included tests of applicable controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated December 2020.

For this audit, we reviewed 6 of 72 judgmentally selected systems in USAID's inventory as of October 16, 2023. We conducted our work from September 15, 2023, to June 26, 2024. Audit fieldwork covered USAID's headquarters located in Washington, DC, and included eight overseas missions for certain tests.

Our audit was performed in accordance with generally accepted government auditing standards, as specified in Government Accountability Office's 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 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. However, we found weaknesses in USAID's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in four of nine Inspector General FISMA Metric Domains. We made seven recommendations to assist USAID in strengthening its information security program.

Our findings and recommendations are included in the accompanying report.

Respectfully,

RMA Associates

RMA Associates LLC

Table of Contents

Summary of Results

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an evaluation of the United States Agency for International Development's (USAID) information security program for fiscal year (FY) 2024. The audit 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 sources.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure (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.

FISMA also requires the agency Inspectors General (IGs) to assess the effectiveness of agency information security programs and practices and report the results of the assessments to the Office of Management (OMB). Annually, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) provide instructions to Federal agencies and IGs for assessing agency information security programs.

For FY2024, OMB required IGs to assess 20 core and 17 supplemental IG FISMA reporting metrics. The FY 2024 metrics are designed to assess the maturity[3] of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (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 FISMA reporting metrics.

[3] The five maturity models are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2024 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2024 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

This audit was performed 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. RMA determined that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

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

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured that the hardware and software assets connected to the network were covered by an organization-wide hardware/software asset management capability and were subject to the monitoring processes defined within the organization's Information System Continuous Monitoring (ISCM) strategy.
- Employed automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to USAID's network.
- Measured the effectiveness of its awareness program and monitored qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices.
- Employed automated mechanisms to test system contingency plans more thoroughly and effectively.

As shown in Table 2, the overall maturity of USAID's information security program was Managed and Measurable (Effective).

Table 2: FY 2024 USAID Maturity Level

Cybersecurity Framework Security Functions	Core Metrics	FY 24 Supplemental Metrics	FY 24 Assessed Maturity Level
Identify	Effective	Effective	Managed and Measurable
Protect	Effective	Effective	Managed and Measurable
Detect	Ineffective	Ineffective	Consistently Implemented
Respond	Effective	Effective	Managed and Measurable
Recover	Effective	Effective	Managed and Measurable
Overall	Effective	Effective	**Managed and Measurable**

However, we found weaknesses in USAID's security posture in preserving the Agency's information and information systems' confidentiality, integrity, and availability. Specifically, we noted weaknesses in four IG FISMA Metric Domains (Table 3).

Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2024 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Identify	Risk Management	None
	Supply Chain Risk Management	USAID Needs to Implement a Formal Training Program to Detect Counterfeit System Components (Finding 4).
Protect	Configuration Management	None
	Identity and Access Management	USAID Needs to Resolve Long-Standing Weaknesses in its Access Controls (Finding 1).
	Data Protection and Privacy	None
	Security Training	None
Detect	Information Security Continuous Monitoring	USAID System-Level Security Control Assessments Were Overdue and Monitoring Dashboard Was Not Automated to Reflect the Current System-Level Status (Finding 2). USAID Needs to Timely Review the ISCM Strategy and Establish an Ongoing Lessons-Learned Process (Finding 3).
Respond	Incident Response	USAID Needs to Implement Event Logging Level 3 Requirements Set Forth by OMB M-21-31 (Finding 5).

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Recover	Contingency Planning	None

We are making seven recommendations to address the weaknesses. In addition, as discussed in Finding 1 and summarized in Appendix II, USAID did not implement two of four prior FISMA audit recommendations that were open for almost four years. According to USAID officials, the two recommendations involved multiple business units. The Office of the Chief Information Office was only responsible for a portion of the onboarding and offboarding process, specifically creating and managing user accounts, and the Office of Human Capital and Talent Management was only responsible for onboarding and offboarding employees. This lack of cooperation has led to challenges for the Agency in closing these recommendations. Detailed findings appear in the following section.

Audit Findings

1. USAID Needs to Resolve Long-Standing Weaknesses in its Access Controls.

Cybersecurity Framework Security Function: *Protect*
FY24 IG FISMA Metric Domain: *Identity and Access Management*

In its FY 2020 USAID FISMA audit report, OIG made two recommendations to address the need to improve controls over the off-boarding of staff, including (1) verifying that separated employees' accounts are disabled in a timely manner and (2) maintaining records for off-boarding of staff.[4] However—after almost four years—although Agency officials have tried to implement those recommendations, they have not been successful.

To illustrate, RMA selected a sample of 9 from a population of 104 separated direct hire employees and 1 from a population of 1 contractor who separated from the Agency in FY 2024. User accounts were not disabled within 24 hours of their separation date in accordance with USAID policy for six of the direct hire employees and the one contractor.

Additionally, RMA selected a sample of 9 from a population of 104 direct hire employees who separated from the Agency in FY 2024 and found that the Agency's required exit clearance forms were not completed or properly completed for 5 of the 9 employees. Specifically, two of the exit forms could not be provided, two were not signed, and one was signed two months after the user's separation date. That form identifies to which systems the employees have access and includes a signed certification that a request has been made to remove access to those systems.

USAID Automated Directives System (ADS) 590.3.10.1 states:

> For audit recommendations that have been resolved (i.e., agreement on action to be taken) by the Agency and an audit organization, it is the Agency's policy to complete corrective action in an expeditious manner that ensures compliance with identified dates for both performance and financial audits.

Further, ADS 590.3.10.2 states, "An audit recommendation should be closed/implemented within one year of the Final Audit Report Date, to the extent possible."

Agency management acknowledged there was not a process in place to verify that separated employee's accounts were disabled timely or that employees and contractors were off boarded in accordance with USAID policy. Agency officials explained that the off-boarding process is complex due to the number of hiring mechanisms, such as U.S. direct hires, contractors, detailees, foreign service nationals, and presidential appointees. Off-boarding hiring mechanisms can involve not only the Offices of the Chief Information Officer and Human Capital Talent Management, but contracting officer's representatives, executive officers, and others as well.

However, according to Agency officials, despite repeated efforts, they have not been able to get

[4] Recommendations 2 and 3 from *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (A-000-21-004-C).

those other offices to take the action needed to implement the two long-standing recommendations. Yet, Agency officials did not elevate these weaknesses as significant deficiencies[5] to their cognizant Management Councils on Risk and Internal Control, which are responsible for providing management and oversight of its enterprise-level risk and control weaknesses and submitting an annual Federal Managers' Financial Integrity Act[6] certification[7] to the Agency-level control council.

Without ensuring accounts are timely disabled upon staff's separation from the Agency, USAID is at an increased risk of account misuse and unauthorized access, thus making it difficult for the Agency to meet the zero trust requirements, as mandated by OMB.[8] Further, without ensuring that separating staff complete exit forms and are off-boarded properly, the Agency is at increased risk of information technology equipment, including laptops, tablets, cellphones, and other items not being returned. In addition, the Agency lacks assurance that diplomatic passports have been returned, outstanding debts have been paid, and transit benefits have been stopped among other items that are included in exit clearance forms. Due to the significance of these weaknesses and the difficulty the Agency has had in remediating them, we are making the following recommendations.

Recommendation 1: *We recommend that USAID's Chief Information Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not timely disabling network accounts for separated employees and contractors, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 2.*

Recommendation 2: *We recommend that USAID's Chief Human Capital Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not maintaining records evidencing that staff have been off-boarded in accordance with Agency policy, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 3.*

[5] USAID defined significant deficiency as "a deficiency or a combination of deficiencies in internal control that in management's judgment, need to be communicated to the next level of management because they represent significant weaknesses in the design or operation of an administrative, programmatic, operational, accounting, or financial internal control that could adversely affect overall internal control objectives."

[6] The Federal Managers' Financial Integrity Act of 1982 (P.L. 97-255) provides the statutory basis for management's responsibility for and assessment of accounting and administrative internal controls.

[7] According to ADS 596.3.2, certifications must describe significant deficiencies "that could adversely affect" a unit's "ability to meet its internal control objectives."

[8] OMB memorandum M-22-09, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*, January 26, 2022, was issued to "reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. That memorandum requires agencies to meet certain requirements by the end of FY 2024.

2. USAID System-Level Security Control Assessments Were Overdue and Monitoring Dashboard Was Not Automated to Reflect the Current System-Level Status.

Cybersecurity Framework Security Function: *Detect*
FY24 IG FISMA Metric Domain: *Information Security Continuous Monitoring*

USAID did not consistently conduct system-level security assessments on an annual basis for four of the six systems selected for testing. USAID's last control assessment was completed in 2022. Since then, USAID has not performed the annual assessment of one-third of the system controls as required by their policy. In addition, USAID's continuous monitoring (ConMon) dashboard did not accurately reflect system grades and performance measures. Moreover, the ConMon dashboard did not include notes alerting reviewers that control assessments for the four systems had not been performed and why the system scores did not reflect that the assessments had not been performed.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

> **CA-2 CONTROL ASSESSMENTS**
> Control:
> […]
> d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

USAID's *Information Security Continuous Monitoring (ISCM) Strategy*, Version 7.0, April 6, 2022, states:

> 7.1 Security Control Assessments (Cybersecurity and Privacy)
>
> USAID "Core Controls" are those controls that are most important to the organization and associated systems and should be assessed annually. The Agency also requires that at least one-third of the total system controls be assessed annually, and each control be assessed at least once during every 3-year cycle. This approach eliminates the requirement to perform a complete reassessment of each control every third year. Therefore, a subset of system controls must be selected annually to be assessed.

According to USAID officials, there was a strategic decision made by the leadership to not perform the one-third testing and downgrade the system scores on the ConMon dashboard. The ConMon monitoring dashboard was manually updated by management and did not automatically capture the correct status of control assessments and system scoring. Further, they explained that they did not change the status of the control assessments in the dashboard because they did not want to penalize system owners for not performing the assessments while the Agency transitioned from NIST SP 800-53, Rev. 4 to Rev. 5. They added that they did not have the resources to perform the control assessments and to transition system security controls from Rev. 4 to Rev. 5 at the same time. However, the Agency did not document the deviation from its policies or its acceptance of the risk of not conducting these assessments. Moreover, USAID did not have procedures to document deviations from Agency policy and to accept the risk of such deviations.

Without consistently reviewing and documenting ongoing monitoring and control assessment for USAID systems, Agency stakeholders may not be aware of security and privacy risks to the systems. This may impact the overall risk exposure to the compromise of confidentiality, integrity, and availability of USAID data and information systems. In addition, without an automated enterprise-wide dashboard to provide top management with complete, accurate, and timely information it needs to be aware of enterprise-wide information technology risks, USAID may not be able to anticipate and be protected from threats to confidentiality, integrity, and availability of information and systems in a timely manner.

Recommendation 3: *We recommend that USAID's Chief Information Officer develop and implement procedures to document deviations from Agency policy on security control assessments, including acceptance of the risk of such deviations.*

Recommendation 4: *We recommend that USAID's Chief Information Officer implement accurate automated dashboards to provide enterprise-wide metrics to inform top management of its information technology risks.*

3. USAID Needs to Timely Review the ISCM Strategy and Establish an Ongoing Lessons-Learned Process

Cybersecurity Framework Security Function: *Detect*
FY24 IG FISMA Metric Domain: *Information Security Continuous Monitoring*

USAID did not annually review and update its enterprise-wide *Information Security Continuous Monitoring (ISCM) Strategy*. The ISCM Strategy was updated in April 2022, but not updated and approved again until March 2024—nearly two years after the previous update.

NIST SP 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy* states:

> […] to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high-impact systems. Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems within the organization.

USAID's *Information Security Continuous Monitoring (ISCM) Strategy*, Version 7.0, April 6, 2022, states:

> USAID is required to have both a vibrant Privacy Continuous Monitoring (PCM) and ISCM Program, with effective strategies updated annually.

USAID did not have a process and monitoring mechanism to oversee and track the progress of the ISCM Plan's annual reviews. There was also no ongoing process for documenting lessons learned to make improvements to the ISCM Strategy. The absence of oversight by the assigned parties led to a lapse in the reviews and periodic updates. An outdated or inaccurate ISCM increases the risk of USAID being vulnerable to escalating threats. Such vulnerabilities and attack vectors may not be adequately accounted for in an outdated or inaccurate plan, leaving USAID vulnerable to cyberattacks and data breaches. In addition, without a formal, disciplined lesson-learned process, USAID may not capture information from previous practice and actual risk events, and thereby lose the opportunity to strengthen USAID's security posture.

Recommendation 5: *We recommend that USAID's Chief Information Officer establish and implement a process to track the progress of conducting annual reviews and related lessons learned from the implementation of its* Information Security Continuous Monitoring Strategy.

4. USAID Needs to Implement a Formal Training Program to Detect Counterfeit System Components.

Cybersecurity Framework Security Function: *Identify*
FY24 IG FISMA Metric Domain: *Supply Chain Risk Management*

NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

> **SR-11 COMPONENT AUTHENTICITY**
> Control Enhancements:
> (1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

USAID's *Automated Directives System Chapter 545,* March 28, 2023, Section 545.3.20.8 states that the Senior Accountability Official for Supply Chain Risk Management (SCRM) must ensure that*:*

> SCRM team members are trained to detect counterfeit system components (e.g., hardware, software, and firmware)

USAID did not have formal counterfeit training for designated personnel to effectively identify counterfeit system components, including hardware, software, and firmware—which would be updated regularly to address emerging threats. Agency officials were not aware of the importance of counterfeit detection and prevention within USAID's security framework. The absence of trained personnel significantly increases the risk of counterfeit components being introduced into USAID systems. This can lead to compromised system integrity, the potential introduction of malicious code, and diminished trust in USAID's operational security.

Recommendation 6: *We recommend that USAID's Chief Information Officer establish a formal training program in counterfeit component detection to educate responsible personnel. The training should cover identifying counterfeit hardware, software, and firmware components and should be updated regularly.*

5. USAID Needs to Implement Event Logging Level 3 Requirements Set Forth by OMB M-21-31.

Cybersecurity Framework Security Function: *Respond*
FY24 IG FISMA Metric Domain: *Incident Response*

During audit fieldwork, USAID did not implement event logging (EL) requirements to meet the EL3 (advanced) level, in accordance with OMB memorandum M-21-31, dated August 27, 2021. USAID was required to reach EL3 maturity by August 2023 or within 24 months of the memorandum issuance. As of May 17, 2024, or 33 months since issuance, USAID was at maturity EL2 (intermediate) level.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, states:

> Section I: Maturity Model for Event Log Management
>
> Tier EL3, Rating – Advanced
>
> The agency and all its components meet the following requirements, as detailed in Table 4 (EL3 Advanced Requirements) within Appendix A (Implementation and Centralized Access)
> - Meeting EL2 maturity level
> - Advanced Logging Categories
> - Logging Orchestration, Automation, and Response – Finalizing Implementation • User Behavior Monitoring – Finalizing Implementation
> - Application Container Security, Operations, and Management
> - Advanced Centralized Access
>
> Section II: Agency Implementation Requirements
>
> Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
>
> - [...]
> - Within two years of the date of this memorandum, achieve EL3 maturity.

RMA conducted walkthrough meetings in March 2024, and the subject matter expert (SME) presented that USAID was at level 2. However, in May 2024 after a deadline for providing documents had passed, USAID officials stated that the Agency had met the EL3 maturity level. The officials explained that their event logging checklists lacked details to show the EL3 level's applicability. Therefore, they said that the SME had misinterpreted the checklists by marking entries related to a mainframe as non-compliant with EL3 when they should have been marked as not applicable, thus misreporting the status of the logs. Since the deadline for providing documents had passed, RMA did not verify the official's statement, or the additional documents provided.

By not meeting the logging requirements at maturity EL3 (advanced), USAID decreases its ability to ensure the highest-level security operations center and accelerate incident response efforts to enable more effective defense of Federal information. Therefore, we are making the following recommendation to help USAID to meet EL3 requirements.

Recommendation 7: *We recommend that USAID's Chief Information Officer update the event logging checklist to include details of event logging level 3 (advanced) applicability and implement requirements as specified by the Office of Management and Budget Memorandum M-21-31.*

Evaluation of Management Comments

In response to the draft FISMA report, USAID agreed with recommendations 1 and 3-7, and partially agreed with recommendation 2. We acknowledge management decisions on each of the seven recommendations. USAID's comments, excluding the attachments, are included in their entirety in Appendix III.

USAID outlined its plans to address recommendations 1 and 2. Therefore, we consider recommendations 1 and 2 resolved but open pending completion of planned activities.

USAID stated they completed the final action and requested closure of recommendations 3-7 upon issuance of the final report. For recommendation 6, based on our evaluation of the Agency's comments and review of the evidence provided, we agree that management established a formal training program in counterfeit component detection to educate responsible personnel. Therefore, we consider recommendation 6 closed. However, for recommendations 3, 4, 5, and 7, additional detailed tests are needed to confirm whether the controls are consistently applied and functioning as intended. Therefore, we consider recommendations 3, 4, 5, and 7 to be resolved but open pending verification of the agency's final action.

Appendix I – Scope and Methodology

Scope

RMA conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit was conducted for FY 2024 and tested the core and supplemental metrics identified in the *FY 2023-2024 IG FISMA Reporting Metrics* issued by OMB and the CIGIE.

The scope of this audit was to assess whether USAID's information security program was consistent with FISMA, and the reporting instructions issued by OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). In addition, the audit included tests of security and privacy controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, updated December 2020. We assessed USAID's performance and compliance with FISMA in the following control areas:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

We conducted a risk assessment to identify a representative number of systems (a minimum of 4 internal and 2 external) to be tested when needed for system-level testing. Only moderate systems not previously tested in the prior year were selected for FY 2024. Six out of 72 internal and external systems were selected for testing for FY 2024 from USAID's system inventory dated October 16, 2023.

The audit also included a follow-up on four prior audit recommendations[9,10] to determine if USAID had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for the status of recommendations for the prior year.

[9] Recommendations 1 and 2 in *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report A-000-23-004-C, September 8, 2023).

[10] Recommendations 2 and 3 in *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).

We conducted our work from September 15, 2023, to June 26, 2024. It covered the period from October 1, 2023, through June 26, 2024. Audit fieldwork covered USAID's headquarters in Washington, DC. In addition, the following overseas missions were included in our samples: Afghanistan, Ukraine, Guatemala, Germany, Central Asia, Kosovo, Honduras, and the Democratic Republic of the Congo. Our vulnerability scans covered USAID's headquarters and the following three overseas missions: Honduras, the Democratic Republic of the Congo, and Ukraine.

Methodology

To determine if USAID implemented an effective information security program, RMA conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, RMA reviewed documentation supporting the information security program. These documents included but were not limited to USAID's (1) risk management policy, (2) configuration management procedures, (3) identity and access control measures, (4) security awareness training, and (5) continuous monitoring controls. RMA compared documentation against requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls, including a vulnerability assessment, to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations from FY 2023 and FY 2020.

In testing the effectiveness of the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them. RMA considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, RMA tested samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

Appendix II - Status of Prior Year Recommendations

The following table provides the status of the FY 2023 and FY 2020 FISMA audit recommendations.[11, 12]

Table 4: FY 2023 & 2020 FISMA Audit Recommendations

Audit Report & Recommendation No.	Audit Recommendations	USAID's Corrective Action Plan	USAID's Position	Auditor's Position on the Status
A-000-23-004-C (Rec.1)	We recommend that USAID's Chief Information Officer formally document and implement a revised policy for maintaining a system component inventory to include the specific physical location of agency hardware assets.	USAID's Office of the Chief Information Officer (OCIO) has taken action to update several Standard Operating Procedures (SOPs) to address the issue of tracking specific physical locations of agency hardware assets. USAID concluded an exercise to update all assets within the agency to include as specific as possible, the exact location of the asset. A ServiceNow export of all USAID hardware assets reflects the results of this exercise.	Closed	Agree

[11] *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report A-000-23-004-C, September 8, 2023).

[12] *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).

Audit Report & Recommendation No.	Audit Recommendations	USAID's Corrective Action Plan	USAID's Position	Auditor's Position on the Status
A-000-23-004-C (Rec.2)	We recommend that USAID's Chief Information Officer fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.	USAID has progressively adhered to meeting the EL 1 and 2 requirements by successfully ingesting 100% of EL 1 and EL 2 logs within Splunk. In addition to this automated solution to ingest logs, USAID maintains a manual tracker which tie each of the EL1 and EL2 requirements at the application level to specific ServiceNow tickets that can be reviewed to validate that the logs are being appropriately ingested into Splunk. In addition, OCIO personnel performed walkthroughs with OIG and FISMA auditor personnel on February 28th and March 4th to demonstrate these capabilities, where USAID were informed at the time that the auditors concurred that USAID have met the appropriate EL1 and 2 logging requirements.	Closed	Agree

Audit Report & Recommendation No.	Audit Recommendations	USAID's Corrective Action Plan	USAID's Position	Auditor's Position on the Status
A-000-21-004-C (Rec.2)	We recommend that 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.	OCIO engaged in a collaborative effort 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 USAID policy. This collaboration led to the Implementation of a Launchpad based process within the existing ServiceNow Human Resources Service Delivery (HRSD) module. Within LaunchPad, a user separation request is initiated for employees leaving this agency either by the employee or their supervisor or Administrative Management Services (AMS) officer. The AMS officer submits the de-activation of their System access to OCIO for final removal of access. It is the AMS officers responsibility to ensure the employee's account and system access (except for Classnet/OpenNet) are terminated. A task is generated for the AMS Officer to submit the systems/account deactivation. ServiceNow automatically creates a ticket to track these activities, which includes disabling the user's account. Once the ticket is created, a member of OCIO staff is assigned the responsibility of disabling the user's account within an established timeframe in order to complete the offboarding process.	Closed	Disagree. See finding 1.

Audit Report & Recommendation No.	Audit Recommendations	USAID's Corrective Action Plan	USAID's Position	Auditor's Position on the Status
A-000-21-004-C (Rec.3)	We recommend that USAID's Chief Human Capital Officer should implement a process to maintain records electronically for onboarding and offboarding staff.	Onboarding: OCIO), in collaboration with HCTM's Onboarding Team, developed the Work-Ready Progress Dashboard, which pulls together Navigate and Service Central Data all into one easy-to-view dashboard. The dashboard creates visibility across the onboarding process, from tentative offer to being work-ready, so the viewer knows exactly in which phase the candidate is in at any given time. Offboarding: ● Hire an Offboarding Supervisor with responsibility for managing the offboarding process and liaising with stakeholders end-to-end. ● Establish working partnerships with all offboarding stakeholders. ● Enhance the Offboarding Tool with stakeholders' input and validation to address needs. ● Enact a change management strategy that will both ensure a smooth transition in using the enhanced tool and consider governance and sustainability. ● Commit to a hypercare period following release of the enhanced tool.	Closed	Disagree. See finding 1.

Appendix III – Management Comments

MEMORANDUM

TO: Toayoa Aldridge, Assistant Inspector General for Audits, Inspections, and Evaluations

FROM: Chief Information Officer, Jason Gray /S/

DATE: August 30, 2024

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 2024 but Long Standing Weaknesses Persist* (Task No. AA150423)

The U.S. Agency for International Development (USAID) would like to thank the Office of Inspector General (OIG) for the opportunity to provide comments on the subject draft report (Tab 2). The Agency partially agrees with the recommendations, herein provides plans for implementing them, and reports on significant progress already made.

USAID is committed to supporting improvements to managing our information security program as required by the Federal Information Security Modernization Act of 2014 (FISMA). The OIG acknowledges this commitment in the draft report, by recognizing that our agency had generally implemented an effective agency-wide information security program in Fiscal Year 2024.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE REPORT RELEASED BY THE USAID OFFICE OF THE INSPECTOR GENERAL (OIG) TITLED, *USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Long Standing Weaknesses Persist* (Task No. AA150423)

Please find below the management and technical 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 7 recommendation(s) for USAID:

Recommendation 1: We recommend that USAID's Chief Information Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not timely disabling network accounts for separated employees and contractors, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 2.

- **Management Comments:** M/CIO agrees with the recommendation. As discussed with OIG during the exit conference, M/CIO plans to report this recommendation as a control deficiency to the agency Risk Management Council (RMC), for inclusion on the Agency Risk Profile. The RMC is co-chaired by the Deputy Assistant Administrators (DAAs) from the Bureaus for Management (M) and Policy, Learning, and Resource Management (PLR), and is responsible for assessing the roll-up of enterprise risks, based on input from Bureau and Independent Office (B/IO) level Management Councils on Risk and Internal Control (MCRICs). This approach will enable M/CIO to more closely collaborate with other stakeholders within the agency who have shared responsibilities over agency workforce processes, and present this issue as a risk at the Agency-level to the Executive Management Council on Risk and Internal Control (EMCRIC). The EMCRIC is chaired by the Deputy Administrator, or designee, and is the most senior body charged with reviewing and providing penultimate approval of the Agency's Risk Profile, and proposed corrective measures or risk response.

- **Target Completion Date:** December 31, 2025

Recommendation 2: We recommend that USAID's Chief Human Capital Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not maintaining records evidencing that staff have been off boarded in accordance with Agency policy, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 3.

- **Management Comments:**

  HCTM partially agrees with this recommendation. HCTM plans to report this recommendation as a control deficiency to the Agency Risk Management Council (RMC), for inclusion on the Agency Risk Profile. HCTM does not agree that this significant deficiency should be mitigated and tracked by the HCTM MCRIC alone. HCTM will work with partners across the agency on systemic challenges that have prevented HCTM from maintaining proper offboarding records within a strict timeline. These efforts will be bound by resource constraints, which may also affect the target completion date.

As a priority corrective action, HCTM will better educate employees on their offboarding responsibilities. This will take the form of an automated email from the offboarding tool that is triggered once they have submitted their intention to leave the Agency, which will provide an overview video or one-pager about the offboarding process and instructions about how to use the offboarding tool.

HCTM will work with t AMS and EXO Officers to think about how the Agency can operate from a standard set of offboarding instructions, procedures, and timelines across the Bureaus, Independent Offices and Missions (B/IO/M).

HCTM will continue to review process efficiencies, to streamline timelines from when HCTM signs off on exit clearance packages once all clearing officials have signed off to when HCTM forwards the exit clearance package to the Bureau for Management, Office of the Chief Financial Officer, Payroll Office. The Payroll Office then has eight weeks upon receipt to perform its offboarding functions such as processing leave pay-outs and collecting outstanding debts.

- **Target Completion Date:** August 29, 2025

Recommendation 3: We recommend that USAID's Chief Information Officer develop and implement procedures to document deviations from Agency policy on security control assessments, including acceptance of the risk of such deviations.

- **Management Comments:** M/CIO agrees with the recommendation and has taken actions to address it. M/CIO has developed and implemented a process which requires a System Owner or designee to complete the IA Security Risk Decision Form (Tab 3) to request and document a risk acceptance decision or an exception of a known deficiency. The form is required to include the justification and the compensating control(s), and is submitted to the Authorizing Official and Chief Information Security Officer for approval.

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

Recommendation 4: We recommend that USAID's Chief Information Officer implement accurate automated dashboards to provide enterprise-wide metrics to inform top management of its information technology risks.

- **Management Comments:** USAID M/CIO agrees with the recommendation and has taken actions to address it. Prior to the audit, M/CIO made a risk based decision to deviate from the normal metric collection for updating its dashboards. Specifically, we were not downgrading systems for not completing annual assessments on time due to our focus on completing full NIST 800-53 rev. 5 assessments. We have since reverted back to our normal metric collection and scoring, which includes negatively impacting systems on the automated dashboards for not conducting annual assessments. This is evidenced by the updated dashboard (Tab 4) which shows systems having the appropriate scores for not completing an annual assessment to date.

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

Recommendation 5: We recommend that USAID's Chief Information Officer establish and implement a process to track the progress of conducting annual reviews and related lessons learned from the implementation of its Information Security Continuous Monitoring Strategy.

- **<u>Management Comments</u>:** M/CIO agrees with the recommendation and has taken actions to address it. M/CIO has updated and implemented the Information Security Continuous Monitoring (ISCM) Strategy (Tab 5). This document describes the Agency strategy for ISCM, which includes the NIST Risk Management Framework requirement for the continuous monitoring of security control effectiveness and any proposed or actual changes to information systems (ISs) and their environment of operation. The strategy includes the NIST Continuous Monitoring Phase, defined as all security control activities that apply to the FISMA inventory of ISs, privacy continuous monitoring requirements, as well as guidance on metrics and on the use of a maturity model to report FISMA metrics. Section 7, *Continuous Monitoring Ongoing Actions*, describes the requirements and process for conducting and tracking annual control assessments; and Section 8, *Lessons Learned*, documents the improvements made to the ISCM program since the strategy's last review and update**.**

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

Recommendation 6: We recommend that USAID's Chief Information Officer establish a formal training program in counterfeit component detection to educate responsible personnel. The training should cover identifying counterfeit hardware, software, and firmware components and should be updated regularly.

- **<u>Management Comments</u>:** M/CIO agrees with the recommendation and has taken actions to address it. On May 15, 2024 M/CIO issued the *Memorandum to Designate Role-Based Anti-Counterfeit Training* (Tab 6). This memo requires personnel that are in the following positions to take the role-based Anti-Counterfeit Training by July 1, 2024 with an annual refresher:
  - Personnel working in the USAID Warehouse with responsibilities related to the receipt, processing, and distribution of government-furnished equipment and IT hardware like laptops, servers, switches, routers, and phones.
  - Personnel with the administrative rights/elevated privileges to install, deploy, patch, or update software or firmware onto GFE or USAID networks (those working within M/CIO/ITO).

  As a result of this memo and its implementation, M/CIO developed and implemented the *Prevention and Detection of Counterfeit Hardware and Software Training* course

(Tab 7), and identified 364 individuals within the agency that were required to take this training annually. As of August 1, 2024, 363 (99.7%) of the 364 identified personnel have taken the training. The remaining individual is currently on extended leave and will take the training upon their return.

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

Recommendation 7: We recommend that USAID's Chief Information Officer update the event logging checklist to include details of event logging level 3 (advanced) applicability and implement requirements as specified by Office of Management and Budget Memorandum M-21-31.

- **Management Comments:** M/CIO agrees with the recommendation and has taken actions to address it. USAID has achieved EL3 on all FISMA systems based on the Office of Management and Budget Memorandum M-21-31 logging definitions and additional required components. M/CIO has updated our internal event logging checklist (Tab 8) to include the details of EL3 applicability for each system. Where EL3 requirements are not applicable, we have documented the associated justification, and where EL3 requirements are applicable, we have documented the source for how we have implemented requirements as specified by OMB M-21-31.

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