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

FISMA: USAID Implemented an Effective Information Security Program Through April 14, 2025, Despite Some Concerns

Report A-000-26-004-M
March 4, 2026

Evaluation

Office of Audits, Inspections, and Evaluations

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

DATE: March 4, 2026

TO: Eric Ueland
Performing the Duties of Administrator and Chief Operating Officer
U.S. Agency for International Development

FROM: Gabriele Tonsil /s/
Acting Assistant Inspector General for Audits, Inspections, and Evaluations

SUBJECT: FISMA: USAID Implemented an Effective Information Security Program Through April 14, 2025, Despite Some Concerns

This memorandum transmits the final report on our evaluation of USAID's information security program for fiscal year 2025, in support of the Federal Information Security Modernization Act of 2014 (FISMA). Our objective was to determine whether USAID implemented an effective information security program.

USAID did not have any comments on the draft report.

The report contains five new recommendations related to USAID's information security program and identified four prior FISMA audits recommendation that USAID has not yet implemented. We consider all five of the new recommendations open and unresolved, two of the prior recommendations open and unresolved, and the other two prior recommendations open and resolved. Please provide us with a management decision for each of the five new recommendations, including agreement or disagreement with the recommendation and a plan and target date for corrective action, copying the Audit Performance and Compliance Division.

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

Contents

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

Report No. A-000-26-004-M
March 4, 2026

Report in Brief

Why We Did This Evaluation

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. The Federal Information Security Modernization Act of 2014 (FISMA) requires the U.S. Agency for International Development (USAID) to implement policies and procedures to protect its information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. The act also directs the USAID Office of Inspector General (OIG) to conduct an annual independent assessment of the Agency's information security programs practices and report the results of the assessment to the Office of Management and Budget.

On March 28, 2025, the Secretary of State announced that USAID would cease operating as an independent agency. For now, the Agency will continue to be responsible for certain IT systems and its information security program.

In accordance with FISMA, we conducted this evaluation to determine whether USAID had implemented an effective information security program. We focused on USAID's information security program for fiscal year 2025 through April 14, 2025, the last day USAID staff provided information to us due to the transfer of certain Agency functions to the Department of State.

What We Recommend

We made five recommendations to USAID to perform risk and security control assessments for two systems, include cybersecurity duties in position descriptions and performance plans, develop and implement policies and procedures for maintaining data and metadata inventories, and implement network monitoring and enforcement mechanisms. We also referenced four prior recommendations the Agency has not implemented.

What We Found

USAID implemented an effective information security program as of April 14, 2025. For example, USAID used secure configurations for its information systems, ensured that administrative accounts were compliant with Agency policies and procedures, implemented processes for responding to incidents and its contingency plans, and effectively mitigated software vulnerabilities on its network. Although we could not assess the effectiveness for the full fiscal year, we identified certain required actions USAID failed to take but could not determine the reasons why due to the unavailability of responsible Agency staff.

USAID did not perform risk assessments and security controls assessments for two of six selected systems as required. Inconsistent risk assessments can impact an agency's ability to effectively manage cybersecurity risks, respond to threats to its system security environment, and identify vulnerabilities and weaknesses in the security posture.

USAID could not demonstrate that it had formalized cybersecurity duties, policies for maintaining data inventories, or mechanisms for network monitoring and enforcement. As a result, USAID faced the risk that sensitive data might be lost or misused, which could result in legal action and reputational harm. The Agency also increased the risk of miscommunication, unaddressed security gaps, and vulnerabilities across its information technology environment. Finally, without monitoring and enforcement mechanisms, the Agency may not have been able to quickly mitigate the risks from noncompliant devices.

USAID did not implement four of eight prior OIG recommendations pertaining to disabling network accounts and maintaining records for offboarded staff.

Introduction

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) directs OIG to annually assess the effectiveness of the U.S. Agency for International Development's (USAID) information security program and practices and report the results of the assessments to the Office of Management and Budget (OMB).

On March 28, 2025, the Secretary of State announced that USAID would cease operating as an independent agency, and on July 1, 2025, the Department assumed responsibility for many of the Agency's functions and its ongoing programming. Remaining USAID personnel are responsible for managing the closeout of terminated awards and the wind down of the Agency's independent operations. According to a senior Agency official, USAID will continue to be responsible for certain IT systems and its information security program until the wind down is complete.

In accordance with FISMA, we conducted this evaluation to determine whether USAID had implemented an effective information security program.[1] Our review focused on USAID's information security program for fiscal year (FY) 2025 through April 14, 2025, the last day USAID staff provided information to us. As a result, we were unable to provide an assessment on the status of USAID's information security practices for the full fiscal year. Also, USAID officials were unavailable to provide additional information or clarification of the support initially provided.

To assess the effectiveness of USAID's information security program, we followed OMB and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) FY 2025 IG FISMA reporting metrics and the *Inspector General FISMA Evaluator's Guide* for our review.[2] We reviewed regulatory requirements and analyzed documentation to assess the effectiveness of the Agency's information security program, including USAID's (1) supply chain and risk management policy, (2) configuration management procedures, (3) identity and access control reports, (4) security awareness training, and (5) continuous monitoring controls reports, including for assets. We compared the documentation against requirements stipulated in the FISMA metrics guidance. We also interviewed officials and contractors in USAID's Office of the Chief Information Officer when possible.

We judgmentally selected 6 of 56 systems in USAID's inventory as of October 8, 2024, for certain tests. We selected one internal system because it supported other Agency systems, putting those other systems at risk if it was not secure. We selected three other internal

[1] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 IG FISMA reporting metrics.
[2] OMB and CIGIE, *FY 2025 Inspector General - Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025, and FY 2025 IG FISMA Metrics Evaluator's Guide, May 5, 2025.

systems and two external systems on a rotation basis to ensure that we evaluated every system that had a moderate effect on the Agency if breached.[3]

We conducted our review from September 2024 to January2026 using CIGIE's *Quality Standards for Inspection and Evaluation*. Appendix A provides more detail on our scope and methodology.

Background

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 requires agency heads to implement policies and procedures to protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

OMB and CIGIE provide instructions on assessing agency information security programs to inspectors general (IGs).[4] To help facilitate these assessments, the instructions contain a set of core and supplemental metrics that IGs must evaluate for FY 2025.

Various requirements are in place to help USAID implement an effective information security program. For example, to maintain a comprehensive and accurate inventory of agency data and corresponding metadata and to prevent loss or pilferage of assets, Federal regulations require agencies to maintain comprehensive and accurate inventories for their various data types, including data from third-party providers.[5] In addition, to secure information systems from bad actors, Federal guidance requires agencies to implement network monitoring and enforcement mechanisms to identify and disconnect noncompliant devices.[6] Further, the IG FISMA reporting metrics require agencies to include significant cybersecurity duties in individuals' position descriptions and performance plans.

Additionally, USAID established requirements to protect its information systems. For example, one policy describes requirements for performing risk assessments of Agency systems, and another describes requirements for assessing the effectiveness of controls for the systems.[7]

[3] The National Institute of Standards and Technology (NIST) defines a moderate effect as "the loss of confidentiality, integrity, or availability [that] could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." NIST, *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standards Publication 199), February 2024.
[4] CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, Version 1.0, May 5, 2025.
[5] Federal Records Act, Subpart B, § 1220.30, under 44 U.S.C. 3101 and IG FISMA reporting metric #10, *Consistently Implemented,* paragraph1.
[6] OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I, Section 4, "Specific Requirements," July 28, 2016.
[7] USAID, Automated Directives System (ADS), Chapter 545, *Information System Security*, Section 545.3.16.3, "Risk Assessment (RA-3)," December 2022; and USAID, *Information Security Continuous Monitoring (ISCM)*, April 6, 2022.

USAID's Chief Information Officer is responsible for overseeing the security posture of information systems. The Chief Information Officer is also responsible for establishing and implementing policies to secure the Agency's systems from bad actors.

In our FY 2024 FISMA audit, our contracted audit firm concluded that USAID generally implemented an effective information security program.[8] However, the firm identified weaknesses and determined that USAID had not yet implemented six new and two prior recommendations at the time the report was issued.

USAID Implemented an Effective Information Security Program Until April 14, 2025, but Concerns Exist With Risk and Control Assessments, Cybersecurity Duties, Data Inventories, and Network Monitoring

USAID implemented an effective information security program in FY 2025 as of April 14, 2025, but we could not determine the effectiveness for the remainder of the fiscal year. Nonetheless, we determined that the Agency did not perform risk assessments and security control assessments for two of the systems we selected. Further, due to the unavailability of staff, USAID could not provide us with evidence that it had formalized cybersecurity duties, policies for maintaining data inventories, or mechanisms for network monitoring and enforcement. In addition, we found that the Agency did not implement four of eight prior recommendations.

USAID Implemented an Effective Information Security Program Through April 14, 2025

USAID implemented an effective information security program in FY 2025 as of April 14, 2025, which was the last day Agency officials responded to our requests. However, Agency officials did not provide documentation about their information security program after that date, and we therefore could not conclude on the effectiveness of the program for the remainder of the fiscal year. Nonetheless, we determined that USAID, for example:

- Used secure configurations for its information systems as required by the National Institute of Standards and Technology (NIST).[9]
- Managed its system administrator accounts in accordance with Agency policies.[10]
- Implemented processes for responding to information security incidents as NIST requires.[11]

[8] USAID OIG, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2024 in Support of FISMA but Longstanding Weakness Persist* (A-000-24-005-C), September 19, 2024.
[9] NIST, Special Publication 800-53 (Revision 5), *Security and Privacy Controls for Information Systems and Organizations*, CM-6, "Configuration Settings," September 2020.
[10] ADS 545, Information System Security, Section 545.3.2.6, "Least Privilege (AC-6)," December 28, 2022.
[11] NIST, Special Publication 800-53 (Revision 5), *Security and Privacy Controls for Information Systems and Organizations*, IR-4, "Incident Handling," September 2020.

- Implemented its contingency plans as NIST requires.[12]
- Effectively mitigated software vulnerabilities on its network as NIST requires.[13]

However, we found certain areas of concern. For example, USAID did not perform updated risk and security controls assessments for two of the six systems, as Agency policies required.[14] The Agency also did not provide evidence that it formalized its cybersecurity duties, documented policies for data inventories, and implemented network monitoring and enforcement mechanisms.

USAID Did Not Perform Risk Assessments for Two of Six Selected Systems

USAID performed an updated risk assessment for four of the six systems we evaluated within a year as required by Agency policy. However, it did not do so for the remaining two systems. The risk assessment for one of those two systems was dated November 21, 2023, which was 8 months overdue. The other risk assessment was dated January 20, 2023, which was 18 months overdue. Agency policy requires USAID to perform a risk assessment at least annually or whenever there are significant changes to the system.[15] Due to the unavailability of responsible Agency staff to provide us with information, we could not determine why the two risk assessments had not been performed since 2023.

Risk assessments are an important tool for identifying and prioritizing risks to Agency information systems, providing crucial information needed to support appropriate responses. Inconsistent risk assessments can impact an agency's ability to effectively manage cybersecurity risks. Specifically, USAID may not have been able to effectively assess, identify, and mitigate information security risks; minimize its vulnerabilities; and respond to threats to its system security environment. In addition, USAID faced the risk of unauthorized access, loss of information, unauthorized changes to systems, and litigation.

USAID Did Not Perform Security Controls Assessments for Two of the Six Selected Systems

USAID performed security controls assessments for four of the six reviewed systems as required but did not do so for the remaining two systems. USAID's information security strategy required the Agency to assess at least one-third of the total system controls annually and to assess each control at least once during every 3-year cycle.[16] Due to the unavailability of responsible Agency staff to provide us with information, we could not determine the underlying causes to show why the Agency failed to assess its security controls as required.

[12] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (CP-4), "Contingency Plan Testing," September 2020.
[13] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SI-7), "Software, Firmware, and information integrity," September 2020.
[14] ADS 545, Information System Security, Section 545.3.16.3, "Risk Assessment (RA-3)," December 2022; and USAID, *Information Security Continuous Monitoring (ISCM) Strategy*, Version 7, Section 7.1, April 2022.
[15] ADS 545, Information System Security, Section 545.3.16.3, "Risk Assessment (RA-3)," December 2022.
[16] USAID, *Information Security Continuous Monitoring (ISCM) Strategy*, Version 7, Section 7.1, April 2022.

Security controls assessments help agencies identify weaknesses in their security posture and actions needed to mitigate them. By inconsistently performing security controls assessments, USAID risked system compromise and loss of sensitive data, which could lead to legal action and reputational harm.

USAID Did Not Provide Evidence That It Formalized Cybersecurity Duties

USAID could not demonstrate that it had established personnel position descriptions and performance plans needed to formalize cybersecurity duties. According to the IG FISMA reporting metrics, each agency should include significant cybersecurity duties in individual position descriptions and performance plans.[17] Due to the unavailability of responsible Agency staff, we could not determine whether USAID formalized these duties and, if not, the underlying causes.

The lack of cybersecurity duties in position descriptions and performance plans meant that USAID staff may not have known who was responsible and accountable for managing cybersecurity risks. This also increased the risk of miscommunication, unaddressed security gaps, and vulnerabilities across the Agency's information technology environment.

USAID Did Not Provide Evidence That It Had Policies for Data Inventories

USAID did not provide evidence that it developed and implemented policies and procedures or established roles for maintaining comprehensive data and metadata inventories, including data from third-party providers.[18] Federal regulations require the head of each government agency to make and preserve records containing comprehensive and accurate inventory of data and corresponding metadata for its various data types, including data from third-party providers.[19] For the reasons mentioned above, Agency officials did not respond to our questions about the lack of evidence for their data inventory policies.

Without policies, procedures, and established roles for maintaining comprehensive data inventories, USAID may have lacked complete inventories of its data and metadata. Accordingly, USAID may not have known how to best protect its data and metadata from unauthorized users. Further, the Agency faced the risk that its data, including sensitive data, might be lost or misused, which could result in legal action and reputational harm.

USAID Did Not Provide Evidence That It Implemented Network Monitoring and Enforcement Mechanisms

Due to the unavailability of Agency staff, we could not determine whether USAID implemented network monitoring and enforcement mechanisms to identify noncompliant devices and

[17] OMB and CIGIE, *FY 2025 Inspector General - Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, Metric #3, April 3, 2025.
[18] NIST defines metadata as information about data, such as its format and security classification. NIST, *Guide to Cyber Threat Information Sharing* (Special Publication 800-150), October 2016.
[19] Federal Records Act, Subpart B, § 1220.30, under 44 U.S.C. 3101 and IG FISMA reporting metrics #10.

manually disconnect or isolate noncompliant devices. Further, we could not determine the reasons for the lack of implementation, if any. Federal guidance requires that agencies monitor their systems to identify and respond to noncompliance with security requirements.[20]

Without monitoring and enforcement mechanisms, USAID may not have been able to quickly mitigate the risks from noncompliant devices, which made the Agency vulnerable to system compromise, loss of sensitive information, legal challenges, and reputational harm.

USAID Did Not Implement Four of Eight Prior FISMA Recommendations

USAID implemented four open recommendations pertaining to automated dashboards of its information technology risks, documenting deviations from Agency policy, conducting annual reviews and security event logging. However, as of October 1, 2024, the Agency had not implemented four recommendations pertaining to disabling network accounts and maintaining records for offboarded staff. Appendix B provides more detail on the status of our prior recommendations.

Conclusion

Despite the changes in its operating environment, USAID had implemented an effective information security program in FY 2025 as of April 14, 2025. However, we identified issues that warrant attention to ensure a robust cybersecurity framework that mitigates risks to systems and sensitive information. Conducting risk and control assessments would have left the Agency better equipped to manage threats and vulnerabilities to its information and systems. Formalizing cybersecurity duties and policies for data inventories and implementing monitoring mechanisms are also critical for ensuring the confidentiality, integrity, and availability of government information and systems and protecting Americans and government resources from bad actors.

[20] OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I, Section 4, "Specific Requirements," July 28, 2016.

Recommendations

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

1. Conduct updated risk assessments for the two systems we identified.
2. Perform security controls assessments for the two systems we identified.
3. Determine whether the Agency included cybersecurity duties in position descriptions and performance plans. If not, take corrective action, including addressing the causes for not doing so.
4. Determine whether the Agency developed and implemented policies and procedures for maintaining data and metadata inventories for its various data types, including data from third-party providers. If not, take corrective action, including addressing the causes for not doing so.
5. Determine whether the Agency implemented network monitoring and enforcement mechanisms to identify and disconnect or isolate noncompliant devices. If not, take corrective action, including addressing the causes for not doing so.

OIG Response to Agency Comments

We provided our draft report to USAID for comments on January 12, 2026. On January 28, 2026, we received the Agency's response. The Agency did not have any comments on the draft report.

We consider all five new recommendations open and unresolved.

Appendix A. Scope and Methodology

We conducted our work from September 2024 through January 2026 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Our objective for this evaluation was to determine whether USAID implemented an effective information security program.

To answer our objective, we followed the FY 2025 IG FISMA reporting metrics and IG FISMA Evaluator's Guide, which provides a baseline of suggested evidence and test steps for FISMA-related evaluations.[21] We also used criteria referenced throughout the metrics, including the NIST Cybersecurity Framework.[22]

Our review focused on USAID's information security program for FY 2025 through April 14, 2025, the last day Agency staff provided information to us. We were unable to provide an assessment on the status of USAID's information security practices for the full fiscal year. Also, USAID officials were unavailable to provide additional information or clarification of the support they initially provided. We conducted our work in Washington, DC.

To determine if USAID implemented an effective information security program, we tested the core and supplemental metrics identified in OMB and CIGIE's FY 2025 IG FISMA reporting metrics.[23] We judgmentally selected 6 of 56 systems in USAID's inventory as of October 8, 2024, for certain tests. We selected one internal system because it provided general support to other Agency systems, which would put those other systems at risk if not secure. We selected three other internal systems and two external systems on a rotation basis to ensure that we evaluated every system that had a moderate effect on the Agency if breached.[24] Due to the nature of our sampling, we are unable to project our results to the entire population of systems. However, we determined that our method for selecting the systems was appropriate for our evaluation objective and that the selection would generate valid, reliable evidence to support our findings and conclusions.

To assess the effectiveness of USAID's information security program, we analyzed regulatory requirements and documentation to ascertain the effectiveness of USAID's information security program covering the functional areas in the NIST Cybersecurity Framework. For example, we reviewed USAID's enterprise risk management plan to determine whether it met the requirements in OMB Circular A-123 for identifying new risks. In addition, we reviewed USAID's vulnerability scan results to determine whether the Agency patched critical and high vulnerabilities as required in Agency procedures.[25] We also interviewed officials and contractors in USAID's Office of the Chief Information Officer when possible.

[21] CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, Version 1.0, May 5, 2025.
[22] NIST, *The NIST Cybersecurity Framework*, Version 2.0, February 26, 2024.
[23] OMB and CIGIE, *FY 2025 Inspector General - Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025.
[24] NIST, *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standards Publication 199), February 2024, defines a moderate effect as "the loss of confidentiality, integrity, or availability [that] could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."
[25] USAID, *Standard Operating Procedure, Vulnerability Management Process*, October 31, 2024.

We reviewed and analyzed USAID's information systems security plan to determine whether information systems in the Agency's inventory were subject to the monitoring processes defined within USAID's continuous monitoring strategy. We reviewed the system security plan to determine if the Agency utilized the ServiceNow assets table to track and identify its hardware assets. We reviewed the Job Aid Standard Operating Procedures (SOP) to validate that the Agency effectively mitigated software vulnerabilities on its network to prevent the execution of unauthorized software. We reviewed risk assessment results for the selected systems to determine if the risk assessments were performed within the stipulated timeframe for the selected systems. We reviewed USAID's Information Security Continuous Monitoring Strategy, software licensing agreements, and Renewals Inventory Report to determine if there were established policies and procedures for maintaining comprehensive data and metadata inventories, including data from third-party providers.

We reviewed the Change Management SOP and change control reports to determine if authorized Agency officials reviewed and approved changes to USAID's information systems. We reviewed the Elevated Privilege Management Request SOP to determine whether the Agency managed its administrative accounts in accordance with stipulated procedures. We reviewed disk encryption configuration settings screenshots to determine if the Agency implemented strong encryption settings. Finally, we inspected USAID's most recent cybersecurity workforce assessment and workforce progress report to determine if the Agency's cybersecurity training was updated based on its risk assessment results.

We reviewed screenshots of continuous monitoring dashboards of USAID's systems and security controls assessment results for the selected systems to determine whether the Agency implemented continuous monitoring in accordance with FY 2025 FISMA reporting metrics. We followed up, but USAID officials were unavailable to provide additional information to confirm that the Agency implemented continuous monitoring as required.

We reviewed the *Cybersecurity and Privacy Incident Management Program Incident Response Playbook* and its most recent incidents reports to determine if USAID implemented processes related to security incident detection, analysis, and response in accordance with the NIST Cybersecurity Framework.

We reviewed USAID's most recent system contingency plan to determine if the Agency tested its information system contingency planning processes in accordance with the NIST Cybersecurity Framework. We also reviewed the Agency business impact analysis to determine if it guided USAID's contingency planning efforts in accordance with the NIST Cybersecurity Framework.

To determine the status of recommendations we made to USAID in our FY 2020 and FY 2024 FISMA audit reports, we reviewed documentation the Agency provided during this FY 2025 evaluation.[26] Appendix B provides details about these recommendations.

[26] 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; and *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2024 in Support of FISMA but Longstanding Weakness Persist* (A-000-24-005-C), September 19, 2024.

Appendix B. Status of Prior Recommendations

The following table provides the status of recommendations from our FY 2020 and FY 2024 FISMA audit reports that were open as of October 1, 2024, the beginning of the evaluation period.[27]

Table 1. Status of Prior Recommendations.

Report & Recommendation #	Recommendation	USAID's Position	Evaluator's Position
A-000-24-005-C (FY 2024, Rec. 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.	Open	Open
A-000-24-005-C (FY 2024, Rec. 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.	Open	Open
A-000-24-005-C (FY 2024, Rec. 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.	Closed	Closed
A-000-24-005-C (FY 2024, Rec. 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.	Closed	Closed
A-000-24-005-C (FY 2024, Rec. 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.	Closed	Closed
A-000-24-005-C (FY 2024, Rec. 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.	Closed	Closed

[27] 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; and *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2024 in Support of FISMA but Longstanding Weakness Persist*(A-000-24-005-C), September 19, 2024.

Report & Recommendation #	Recommendation	USAID's Position	Evaluator's Position
A-000-21-004-C (FY 2020, Rec. 2)	We recommend that USAID's Chief Information Officer should collaborate with the Office of Human Capital and Talent Management to document and Document and implement a process to verify that separated employees' accounts are disabled in a timely manner in accordance with USAID policy.	Open	Open
A-000-21-004-C (FY 2020. Rec. 3)	We recommend that USAID's Chief Human Capital Officer should Implement a process to maintain records electronically for onboarding and offboarding staff.	Open	Open

Source: OIG's FY 2020 and FY 2024 FISMA audit reports and USAID's documentation submitted during the FY 2025 evaluation.

Visit our website at oig.usaid.gov and
follow us on social media.

X: @AidOversight
LinkedIn: USAID Office of Inspector General
Instagram: @usaid.oig

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

Report Waste, Fraud, and Abuse
Online Complaint Form