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

FISMA: Overall Effectiveness of USADF's Information Security Program for FY 2025 Could Not Be Determined and Weaknesses Exist

Report A-ADF-26-001-M
January 13, 2026

Evaluation

Office of Audits, Inspections, and Evaluations

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

DATE: January 13, 2026

TO: Elisabeth Feleke
Chief Program Officer
U.S. African Development Foundation

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

SUBJECT: FISMA: Overall Effectiveness of USADF's Information Security Program for FY 2025 Could Not Be Determined and Weaknesses Exist

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

We could not determine the overall effectiveness of USADF's information security program for FY 2025 because Agency staff and documentation were not available to support the evaluation. Nonetheless, we identified areas of concern.

We did not receive comments from USADF on the draft evaluation report. Should we receive written comments from the Agency at a later date, we will update and reissue the report to reflect the comments and technical changes as applicable.

The report contains our findings, five new recommendations, and two recommendations from our FY 2024 FISMA audit that USADF has not yet implemented. We consider all seven recommendations open and unresolved. 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.

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

Contents

Report in Brief 1
Introduction 2
Background 3
OIG Could Not Determine the Overall Effectiveness of USADF's Information Security Program but Identified Areas of Concern 4
OIG Could Not Determine If USADF Implemented an Effective Security Program for FY 2025 4
USADF Did Not Patch Vulnerabilities in a Timely Manner 4
USADF Did Not Finalize Its Enterprise Risk Management Plan 5
USADF's Efforts to Align Cybersecurity Training With Workforce Needs Are Unclear 5
USADF Has Not Implemented Two of the Seven Recommendations From OIG's FY 2024 FISMA Audit 6
Conclusion 6
Recommendations 6
OIG Response to Agency Comments 7
Appendix A. Scope and Methodology 8
Appendix B. Status of Prior Recommendations 10

Report No. A-ADF-25-001-M
January 13, 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. 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) requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems. 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. The act also directs USAID Office of Inspector General to annually assess the effectiveness of the U.S. African Development Foundation's (USADF) information security programs and practices and report the results of the assessments to the Office of Management and Budget.

We conducted this evaluation to determine whether USADF implemented an effective information security program. We focused on USADF's information security program for fiscal year (FY) 2025 as of April 14, 2025, the last day Agency staff provided information for our evaluation. Following the February 19, 2025, executive order, "Commencing the Reduction of the Federal Bureaucracy," USADF's staffing was significantly reduced and nearly all Agency personnel were placed on administrative leave.

What We Recommend

We made five recommendations to strengthen the effectiveness of USADF's information security program. In addition, we referenced two recommendations from our 2024 FISMA audit that the Agency has not yet implemented.

What We Found

OIG could not determine the overall effectiveness of USADF's information security program. This was because nearly all of USADF's staff were placed on administrative leave during our fieldwork and thus could not provide the documentation we needed for our evaluation. Still, we identified the following four areas of concern.

USADF did not patch vulnerabilities in a timely manner. Specifically, 23 critical and 122 high-risk vulnerabilities remained unpatched beyond the 180-day remediation deadline mandated in Agency policy. This increases the risk that malicious actors will cause data breaches, system compromise, and operational disruption in USADF systems.

USADF did not finalize its enterprise risk management plan. This plan would define roles, responsibilities, and authorities for responding to cybersecurity risks. As a result, USADF officials may not know who is responsible for managing cybersecurity risk, which could lead to unaddressed security gaps and vulnerabilities to cyber threats.

USADF's efforts to align cybersecurity training with workforce needs are unclear. The Agency did not provide documentation to show how it evaluated and aligned its annual security training with its workforce's knowledge, skills, and ability to respond to current risks and needs. Thus, the Agency may be unable to fully prepare staff for emerging cybersecurity threats.

USADF has not implemented two of the seven recommendations from OIG's FY 2024 FISMA audit. One recommendation pertains to conducting reinvestigations of staff, and the other focuses on improving information security training.

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 assess the effectiveness of the U.S. African Development Foundation's (USADF) information security programs and practices and report the results of the assessments to the Office of Management and Budget (OMB).

We conducted this evaluation to determine whether USADF implemented an effective information security program.[1] We focused on USADF's information security program for fiscal year (FY) 2025 as of April 14, 2025, the last day Agency staff provided information for our evaluation.

To answer the objective, we followed the FY 2025 FISMA reporting metrics and *FISMA Evaluator's Guide*. Ultimately, we were unable to complete the evaluation procedures needed to answer our evaluation objective due to circumstances beyond USADF's control. Specifically, nearly all of USADF's staff were placed on administrative leave during our fieldwork and could not provide the documentation we needed to complete our evaluation.[2]

Despite this limitation, we were able to perform procedures and assess certain elements of USADF's information security program. To the extent possible, we evaluated evidence to ascertain the effectiveness of controls in place by reviewing USADF's policies and procedures related to information technology, vulnerability scan results, draft enterprise risk management plan, and cybersecurity workforce assessment, among other things. For this evaluation, we judgmentally selected 4 of 12 systems in the Agency's inventory as of October 10, 2024, for certain tests. We selected one system because it was USADF's only internal system and it provided general support to other Agency systems, putting those other systems at risk if it was not secure. We selected the other three systems based on an annual rotation plan to ensure that every system is regularly evaluated.

We conducted our evaluation from September 2024 to December 2025 in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*. Appendix A provides more detail on our scope and methodology.

[1] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 FISMA reporting metrics.

[2] The February 19, 2025, Executive Order 14217, "Commencing the Reduction of the Federal Bureaucracy," required USADF to "reduce the performance of [its] statutory functions and associated personnel to the minimum presence and function required by law." In the following months, USADF's staffing was significantly reduced.

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 entities. 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 the effectiveness of agency information security programs. To help facilitate these assessments, the instructions contain metrics that inspectors general must evaluate for FY 2025.[3]

Various requirements are in place to help USADF implement effective information security programs. For example, the FY 2025 FISMA reporting metrics include a requirement for agencies to perform a workforce assessment, which is used as a basis for improving security training and awareness. Also, USADF's *IT Security Implementation Handbook* establishes Agency policies for its information technology systems.[4] In the handbook, USADF establishes policies for remediating critical and high-risk vulnerabilities, which helps secure its network. In addition, OMB Circular A-123 defines agencies' responsibilities for risk management.[5] It emphasizes that agencies should adopt an enterprise-wide risk management framework for formalizing their plans for responding to cybersecurity risks.

USADF's chief information officer is responsible for overseeing the security posture of the Agency's information systems. The chief information officer is also responsible for establishing and implementing Agency policies to secure its systems from bad actors.

In our FY 2024 FISMA audit, our contracted audit firm concluded that USADF generally implemented an effective information security program.[6] However, the firm found weaknesses in the Agency's supply chain risk management, identity and access management, information security continuous monitoring, and incident response. Based on these findings, we made seven recommendations.

[3] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (version 2.0), April 3, 2025.
[4] USADF, *IT Security Implementation Handbook*, Section 4, "Security and Privacy Program Roles and Responsibilities," February 14, 2025.
[5] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (M-16-17), July 15, 2016.
[6] USAID OIG, *FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-ADF-24-003-C), August 29, 2024.

OIG Could Not Determine the Overall Effectiveness of USADF's Information Security Program but Identified Areas of Concern

Nearly all of USADF's staff were placed on administrative leave during our fieldwork and therefore could not provide the documentation we needed to complete our evaluation. As a result, we could not determine the overall effectiveness of the Agency's information security program for FY 2025. However, we found that USADF did not patch vulnerabilities in a timely manner or finalize its enterprise management plan. In addition, we could not determine the extent to which USADF tailored security training for its workforce due to the unavailability of Agency staff. We also determined that USADF did not implement two of seven recommendations from our FY 2024 FISMA audit.

OIG Could Not Determine If USADF Implemented an Effective Security Program for FY 2025

Since Agency staff had been placed on administrative leave, we could not obtain sufficient, appropriate evidence to fully assess certain information security areas or reach a conclusion on the overall effectiveness of USADF's information security program.

However, we found that certain areas were effective. For example, USADF developed its cybersecurity policies to communicate its cybersecurity objectives, and developed and maintained its hardware inventory, as required by the FY 2025 FISMA reporting metrics.

USADF Did Not Patch Vulnerabilities in a Timely Manner

Our review of USADF's vulnerability scan on December 2, 2024, found that the Agency did not patch critical and high-risk vulnerabilities within the time frames defined in its policy.[7] Specifically, 23 critical and 122 high-risk vulnerabilities remained unpatched beyond the 180-day remediation deadline mandated by USADF's *IT Security Implementation Handbook*.[8] Due to USADF staff's inability to access information, we could not determine the underlying reasons why the Agency did not patch these vulnerabilities in a timely manner.

Hackers are continuously searching for ways to exploit U.S. government network vulnerabilities; thus, software patching, which involves applying changes to software to correct security problems, is a key control.[9] Not patching vulnerabilities increases the risk that the Agency could be exposed to data breaches, system compromise, and operational disruption.

[7] Critical vulnerabilities are the most severe security weaknesses in software, hardware, or systems. These vulnerabilities are highly exploitable, can lead to severe consequences, and affect large number of users or systems. High vulnerabilities are also severe but slightly less critical. They usually are likely to be exploited, can lead to significant consequences, and affect many users or systems.
[8] USADF, *IT Security Implementation Handbook*, Section 4, "Security and Privacy Program Roles and Responsibilities," February 14, 2025.
[9] NIST Special Publication 800-40, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, April 2022.

Further, the failure to mitigate known flaws may allow malicious actors to exploit weaknesses in USADF systems.

USADF Did Not Finalize Its Enterprise Risk Management Plan

We found that USADF did not have a finalized enterprise risk management plan, which contains the Agency's policy for responding to cybersecurity risks. Instead, USADF officials provided us with a draft enterprise risk management plan dated February 5, 2025. According to OMB Circular A-123, agencies should adopt enterprise risk management to identify new risks.[10] Since USADF employees were on administrative leave, we lacked access to the Agency's information and thus could not determine why the enterprise risk management plan remained in draft form.

The lack of formally defined roles, responsibilities, and authorities necessary to manage cybersecurity risk means that USADF staff and leadership may not know who is responsible and accountable for managing cybersecurity risk. This increases the probability of miscommunication, leading to unaddressed security gaps and vulnerabilities to cyber threats across USADF's IT infrastructure.

USADF's Efforts to Align Cybersecurity Training With Workforce Needs Are Unclear

USADF did not provide evidence that it used its workforce assessment results to update its cybersecurity training strategy or plans. Specifically, the Agency did not provide documentation to show how it evaluated and aligned its annual security training with the cybersecurity workforce's knowledge, skills, and ability to respond to current risks and needs. Updating security training with the results of workforce assessments is crucial for ensuring that gaps in USADF staff's knowledge, skills, and abilities are addressed.

According to the FY 2025 FISMA reporting metrics, a workforce assessment should serve as a key input in updating the organization's awareness and training strategy or plans.[11] Training should be aimed at developing and retaining employee knowledge, skills, and abilities and increasing awareness of identified risks and the entity's plan to address risks related to potential changes.

As mentioned above, our inability to interact with USADF staff and access information meant we could not determine the underlying reasons why the Agency did not provide evidence that it used assessment results to update its cybersecurity training strategy or plans for its cybersecurity workforce. Nonetheless, USADF may be unable to account for changing risk environments or align its training programs with actual workforce needs. Further, personnel may lack the specialized knowledge, skills, and abilities required to effectively address current and emerging cybersecurity threats.

[10] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (M-16-17), July 15, 2016.
[11] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (version 2.0), April 3, 2025.

USADF Has Not Implemented Two of the Seven Recommendations From OIG's FY 2024 FISMA Audit

We determined that USADF implemented five of seven recommendations from our FY 2024 FISMA audit but has not yet implemented two recommendations.[12] One of the two recommendations pertains to conducting reinvestigations of Agency staff; the other focuses on improving its information security training. Appendix B provides more detail on the status of our prior recommendations.

Conclusion

As nearly all of USADF's staff had been placed on administrative leave during our fieldwork and could not provide the documentation we required, we could not determine whether the Agency implemented an effective information security program in FY 2025. Nonetheless, having an effective program is essential to mitigate risks to Agency systems and information. Weaknesses in controls to address identified system vulnerabilities, finalize an enterprise risk management plan, and ensure that cybersecurity training aligns with workforce needs—along with unimplemented prior audit recommendations—increase USADF's risk to threats. Strengthening these controls will enhance the Agency's ability to protect the confidentiality, integrity, and availability of its information and systems from cyberattacks and other security risks. Such safeguards address threats to protect Americans and government resources from bad actors.

Recommendations

We recommend that USADF's Chief Information Officer take the following actions:

1. Remediate the 122 high-risk and 23 critical vulnerabilities identified by USADF's December 2, 2024, scans.
2. Evaluate its vulnerability remediation process to determine why high and critical vulnerabilities were not addressed within required time frames and implement corrective actions as appropriate.
3. Finalize the enterprise risk management plan to define roles, responsibilities, and authority for cybersecurity risk management.
4. Determine why the enterprise risk management plan was not finalized and implement corrective action as appropriate.
5. Determine whether USADF updated its cybersecurity training strategy and plans to incorporate the results of the workforce assessments and, if not, update and implement the strategy and plan.

[12] USAID OIG, *FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-ADF-24-003-C), August 29, 2024.

OIG Response to Agency Comments

We provided our draft report to USADF for comment on December 11, 2025. As of December 31, 2025, we had not received a response, and it was unclear when the Agency might provide one. Should we receive comments, we will update and reissue the report to reflect USADF's comments and technical changes as applicable.

We consider all five new recommendations open and unresolved.

Appendix A. Scope and Methodology

We conducted our work from September 2024 to December 2025 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Our objective was to determine whether USADF implemented an effective information security program.[13]

We focused on USADF's information security program for FY 2025 as of April 14, 2025, which was the last day Agency staff provided information for our evaluation. We conducted our work remotely, engaging with staff at USADF's headquarters in Washington, DC, when possible.

To answer our objective, we followed the FY 2025 FISMA reporting metrics and *FISMA Evaluator's Guide*, which provides a baseline of suggested evidence and test steps for FISMA-related evaluations.[14] We also used criteria referenced throughout the metrics, including OMB Circular A-123 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[15] In addition, we used USADF's *IT Security Implementation Handbook* to evaluate the program.[16]

Following the February 19, 2025, executive order, USADF's staffing was significantly reduced, and nearly all Agency personnel were placed on administrative leave.[17] Because we did not have access to USADF officials and certain documentation, we could not assess the Agency's information security program for some areas in NIST's Cybersecurity Framework. For example, USADF did not provide:

- Security plans and assessments for two systems we selected, as discussed below, to determine whether they met requirements in the NIST Cybersecurity Framework.
- Relevant supporting documentation to determine whether the Agency tailored its workforce assessment to account for its changing risks and to update the organization's cybersecurity training.
- Documentation to support whether the Agency implemented processes related to security incident detection and analysis in accordance with the NIST Cybersecurity Framework.
- Documentation to assess to what extent the Agency implemented processes related to security incident handling in accordance with the Framework.

Therefore, we could not determine whether USADF implemented an effective information security program in FY 2025.

[13] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 FISMA reporting metrics.
[14] CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide,* version 1.0, May 5, 2025.
[15] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (M-16-17), July 15, 2016; and NIST, *The NIST* Cybersecurity *Framework (CSF)*, version 2.0, February 26, 2024.
[16] USADF, *IT Security Implementation Handbook*, Section 4, "Security and Privacy Program Roles and Responsibilities," February 14, 2025.
[17] The February 19, 2025, Executive Order 14217, "Commencing the Reduction of the Federal Bureaucracy," required USADF to "reduce the performance of [its] statutory functions and associated personnel to the minimum presence and function required by law."

Nonetheless, we reviewed documentation that USADF officials made available to us to ascertain the effectiveness of certain elements of its information security program and performed some procedures as discussed below.

We judgmentally selected 4 of 12 systems in USADF's inventory as of October 10, 2024, for certain tests. We selected one system because it was USADF's only internal system that provided general support to other Agency systems, which put those other systems at risk if it is not secure. We selected the other three systems based on an annual rotation plan to ensure that every system is regularly evaluated. Due to the nature of our sampling, we were unable to project the results of our samples to the entire population of systems. Nevertheless, we determined that our selection method was appropriate for our objective.

We reviewed documentation, such as USADF's:

- Draft enterprise risk management plan dated February 5, 2025, which was the most current version available at the time of our review. We reviewed that plan to determine whether it met the requirements stated in OMB Circular A-123 for identifying new risks.
- Vulnerability scan results dated December 2, 2024, which was the most recent scanning results as of the date we requested them. We reviewed the scan results to determine whether USADF patched critical and high vulnerabilities within 180 days, as required in USADF's IT Security Implementation Handbook.
- List of approved software to software running on USADF devices to determine whether only approved software was installed on those devices, as required by the Framework.
- Continuous monitoring strategy to determine whether responsible officials were required to log, review, and approve changes in accordance with FY 2025 FISMA reporting metrics.

To the extent possible, we interviewed officials in USADF's Office of the Chief Information Officer responsible for information security programs to gain an understanding of the Agency's implementation of security controls for information systems.

To determine the status of recommendations we made to USADF in our FY 2024 FISMA audit report, we reviewed the Agency's closure requests and supporting documentation.[18] Appendix B provides additional detail on these recommendations.

[18] USAID OIG, *FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-ADF-24-003-C), August 29, 2024.

Appendix B. Status of Prior Recommendations

The following table provides the status of recommendations we made to USADF in our FY 2024 FISMA audit.[19]

Table 1. Prior OIG Recommendations

Recommendation #	Recommendation	USADF's Position	OIG's Position
1	We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether position risk designations are reviewed for all personnel.	Closed	Closed
2	We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether reinvestigations are performed timely for individuals who possess critical-sensitive/high-risk roles that require system access.	Closed	Open
3	We recommend that USADF's Chief Information Officer develop and implement policies and procedures to periodically assess its cybersecurity workforce's knowledge, skills, and abilities to confirm that security training and development activities align with agency needs.	Closed	Closed
4	We recommend that USADF's Chief Information Officer develop and implement policies and procedures for agency personnel to monitor performance metrics for information technology services provided by third parties.	Closed	Closed
5	We recommend that USADF's Chief Information Officer update the change management charter to designate in writing the responsibilities for monitoring performance metrics, conducting lessons-learned activities, and documenting routine updates and minor changes.	Closed	Closed
6	We recommend that USADF's Chief Information Officer update the system security plan to include the frequency for reviewing and updating the contingency plan.	Closed	Closed
7	We recommend that USADF's Chief Information Officer develop and implement policies and procedures to obtain feedback on the agency's specialized security training, update the training program, and request that third-party providers update their training content, as appropriate, to keep current with security practices.	Closed	Open

Note: Although USADF requested closure of Recommendations 2 and 7 from our FY 2024 audit, our review found that the final actions taken did not fully satisfy the intent of the recommendations. Therefore, the two recommendations remain open.
Source: OIG's FY 2024 FISMA audit report and assessment of USADF's recommendation closure requests and supporting documentation.

[19] USAID OIG, *FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-ADF-24-003-C), August 29, 2024.

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