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

USADF Implemented a Managed and Measurable Information Security Program for Fiscal Year 2023 in Support of FISMA

Audit Report A-ADF-23-003-C
September 5, 2023

Information Technology Audits Division

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

MEMORANDUM

DATE: September 5, 2023

TO: USADF, President and Chief Executive Officer, Travis Adkins

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

SUBJECT: USADF Implemented a Managed and Measurable Information Security Program for Fiscal Year 2023 in Support of FISMA (A-ADF-23-003-C)

Enclosed is the final audit report on the United States African Development Foundation (USADF) information security program for fiscal year 2023, 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 CliftonLarsonAllen LLP (CLA) to conduct the audit. The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on USADF's compliance with FISMA. CLA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which CLA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USADF implemented an effective information security program.[2] To answer the audit objective, CLA assessed the effectiveness of USADF's implementation of the FY 2023 IG FISMA Reporting Metrics[3] that fall into the nine domains in

[1] Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 5274, which amends the Inspector General Act of 1978, when USAID OIG contracts with an audit firm to perform the work, USAID OIG provides non-governmental organizations and/or business entities specifically identified in the accompanying report, if any, 30 days from the date of report publication to review the final report and submit a written response to USAID OIG that clarifies or provides additional context for each instance within the report in which the non-governmental organization and/or business entity is specifically identified. Any comments received to this effect are posted for public viewing on https://usaid.oig.gov with USAID OIG's final transmittal. Please direct related inquiries to oignotice_ndaa5274@usaid.gov.

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

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

the following table. Also, CLA assessed USADF's implementation of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

CLA reviewed a sample of 3 of 10 internal and external information systems in USADF's FISMA inventory. Audit fieldwork covered USADF's headquarters located in Washington, DC, from November 30, 2022, to June 15, 2023, for the period from October 1, 2022, through June 15, 2023.

CLA concluded that USADF implemented an effective information security program by achieving an overall Managed and Measurable maturity level based on the FY 2023 IG FISMA reporting metrics. However, as summarized in the table below, CLA noted weaknesses in two of the nine FY 2023 IG FISMA metric domains.

Fiscal Year 2023 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	
Supply Chain Risk Management	
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	

CLA did not make new recommendations because USADF (1) already took action to correct one weakness and (2) did not yet take action to implement an open recommendation for a repeat weakness reported in the FY2021 FISMA audit.[4]

In addition, USADF took final corrective action on the remaining open recommendation from the FY2021[5] FISMA audit. Refer to Appendix III on page 12 of CLA's report for the status of prior year recommendations.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

[4] Recommendation 1 in USAID OIG, "USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA" (A-ADF-22-001-C), November 8, 2021.
[5] Recommendation 3 in USAID OIG "USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA" (A-ADF-22-001-C), November 8, 2021.

United States African Development Foundation's Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2023

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

Director, Information Technology Audits Division
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the United States African Development Foundation's (USADF) information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual review of their agencies' information security program and report the results to the Office of Management and Budget (OMB).

The objective of this performance audit was to determine whether USADF implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA reporting metrics).

For this year's review, OMB required IGs to assess 20 Core IG FISMA reporting metrics and 20 supplemental IG FISMA reporting metrics in the following five security function areas to assess the maturity level and the effectiveness of their agencies' information security program: Identify, Protect, Detect, Respond, and Recover.[1] The maturity levels ranging from lowest to highest are: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. According to the FY 2023 IG FISMA reporting metrics, Managed and Measurable and Optimized are considered effective maturity levels.

The audit included an assessment of USADF's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope included assessing selected security controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA reporting metrics, for a sample of 3 of 10 internal and external systems in USADF's FISMA inventory of information systems.

Audit fieldwork covered USADF's headquarters located in Washington, DC, from November 30, 2022, to June 15, 2023. It covered the period from October 1, 2022, through June 15, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[1] The function areas are further broken down into nine domains.

We concluded that USADF implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2023 IG FISMA reporting metrics. Although we concluded that USADF implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted one weakness in the configuration management domain and another in the identity and access management domain. However, we did not make new recommendations because USADF already took action to correct one weakness and did not yet take action to implement a recommendation from a prior FISMA audit.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our audit to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from USADF on or before September 1, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 1, 2023.

The purpose of this audit report is to report on our assessment of USADF’s compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to the USAID Office of Inspector General.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
September 1, 2023

Table of Contents

SUMMARY OF RESULTS

Background

The United States Agency for International Development (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[2] (FISMA) requirement for an annual evaluation of the U.S. African Development Foundation's (USADF) information security program and practices. The objective of this performance audit was to determine whether USADF implemented an effective information security program.[3]

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

FISMA also requires Agency Inspectors General (IGs) to assess the effectiveness of Agency information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

OMB and the Council of the Inspectors General on Integrity and Efficiency annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA reporting metrics[4] to independently assess their agencies' information security program.

For FY 2023, OMB required IGs to assess the 20 Core Metrics and 20 Supplemental Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program. As highlighted in Table 1, the FY 2023 IG

[2] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of OMB with respect to Agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

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

[4] We submitted our responses to the FY 2023 IG FISMA reporting Metrics to USAID OIG as a separate deliverable under the contract for this audit.

FISMA reporting metrics are designed to assess the maturity of the information security program and align with the five function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2023 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For this audit, we reviewed selected controls[5] mapped to the FY 2023 IG FISMA reporting metrics for a sample of 3 of 10 USADF internal and external information systems[6] in USADF's FISMA inventory as of October 5, 2022.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

We concluded that USADF implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2023 IG FISMA reporting metrics. For example, USADF:

- Maintained an effective enterprise risk management program.
- Implemented an effective personnel security program.
- Maintained an effective information system continuous monitoring program.

Table 2 below shows a summary of the overall maturity levels for each domain and function area in the FY 2023 IG FISMA reporting metrics.

[5] The controls were tested to the extent necessary to determine whether USADF implemented the processes specifically addressed in the IG FISMA reporting metrics. In addition, not all controls were tested for all three sampled information systems because several controls were inherited from USADF's general support system and certain controls were not applicable for external systems.

[6] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Table 2: Maturity Levels for the FY 2023 IG FISMA Reporting Metrics

Security Function	FY 2023 Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Managed and Measurable	**Risk Management**	Optimized
		Supply Chain Risk Management	Consistently Implemented
Protect	Managed and Measurable	**Configuration Management**	Consistently Implemented
		Identity and Access Management	Managed and Measurable
		Data Protection and Privacy	Managed and Measurable
		Security Training	Managed and Measurable
Detect	Optimized	**Information Security Continuous Monitoring**	Optimized
Respond	Optimized	**Incident Response**	Optimized
Recover	Managed and Measurable	**Contingency Planning**	Managed and Measurable
Overall	**Level 4: Managed and Measurable - Effective**		

Although we concluded that USADF implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted one weakness in the configuration management domain and another in the identity and access management domain. (See Table 3.) However, we did not make new recommendations because USADF already took action to correct one weakness and did not yet take action to implement another recommendation from a prior FISMA audit.[7]

Table 3: Weaknesses Noted in the FY 2023 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2023 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	None
	Supply Chain Risk Management	None
Protect	**Configuration Management**	USADF Needs to Continue to Strengthen its Vulnerability and Patch Management Process **(See Finding #1)**
	Identity and Access Management	USADF Did Not Establish a Rules of Behavior to Address Privileged User Responsibilities **(See Finding #2)**
	Data Protection and Privacy	None
	Security Training	None

[7] Recommendation 1, *USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-ADF-22-001-C, November 8, 2021).

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metrics Domain	Weaknesses Noted
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

In addition, USADF took corrective action to close one open recommendation from the FY 2021[8] FISMA audit. Refer to Appendix III for the status of prior year recommendations.

In response to the draft report, USADF agreed with the evaluation results for the FY 2023 IG FISMA reporting metrics and provided a revised date to implement an open prior recommendation. USADF's comments are included in their entirety in Appendix II.

The following section provides a detailed discussion of the audit findings. Appendix I describes the audit scope and methodology.

[8] *USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-ADF-22-001-C, November 8, 2021).

AUDIT FINDINGS

1. USADF NEEDS TO CONTINUE TO STRENGTHEN ITS VULNERABILITY AND PATCH MANAGEMENT PROCESS

Cybersecurity Framework Security Function: *Protect*
FY 2023 IG FISMA Reporting Metric Domain: *Configuration Management*

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* security control SI-2, System and Information Integrity, states the following regarding flaw remediation:

> The organization:
>
> * * *
>
> c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
> d. Incorporates flaw remediation into the organizational configuration management process.

In addition, the *USADF IT Security Implementation Handbook*, section 5 – Vulnerability Monitoring and Scanning RA-5*,* states:

> USADF shall analyze and remediate all findings:
>
> - Critical Vulnerabilities must be addressed within 180 days or as directed by DHS.
> - High Risk Vulnerabilities must be addressed within 180 days or as directed by DHS.
> - Moderate Risk Vulnerabilities must be addressed as time permits per discretion of the Chief Information Security Officer (CISO).
> - Low Risk Vulnerabilities must be addressed within as time permits per discretion of the CISO.
>
> All residual vulnerabilities that cannot be remediated within a provided period shall be documented in the system Plan of Action and Milestones.

CLA's independent vulnerability scans found that no critical or high-risk vulnerabilities were identified outside of USADF's remediation window of 180 days. However, those scans identified medium and low risk vulnerabilities due to missing patches and configuration weaknesses. Specifically, credentialed scans identified 32 medium and 2 low vulnerabilities. Of those, 8 medium and low risk vulnerabilities were also detected in CLA's FY 2022 FISMA scans. Further, 16 medium risk vulnerabilities were also identified in USADF's scans.

In addition, CLA's non-credentialed scans identified 11 medium and 15 low risk vulnerabilities. Of those, 13 medium and 7 low risk vulnerabilities were also identified in CLA's independent scans on the same Internet Protocol addresses in its FY 2022 FISMA scanning.

USADF indicated that, due to resource constraints, they focused resources on remediating critical and high-risk vulnerabilities and on remediating medium and low risk vulnerabilities as time permitted. Although the *USADF IT Security Implementation Handbook* stipulates a timeline to remediate medium and low risk vulnerabilities, there was no process to validate that they were remediated.

By not installing required patches timely and implementing secure configuration settings, there is an increased risk that USADF cannot mitigate the security weaknesses and limit the potential for attackers to compromise the confidentiality, integrity, and availability of sensitive USADF data. Additionally, vulnerabilities can evolve in threat level. Therefore, not addressing medium and low risk vulnerabilities in a timely manner may provide sufficient time for attackers to exploit them and gain access to sensitive data. Delaying remediation of vulnerabilities may increase the risk that an attacker can combine lower risk vulnerabilities with other attacks to increase their exploitation potential.

In a prior report, we made a recommendation for USADF to implement a process for validating that medium and low risk vulnerabilities are remediated in accordance with the agency's policy.[9] Since USADF has not addressed that recommendation, we are not making a new recommendation at this time.

2. USADF DID NOT ESTABLISH RULES OF BEHAVIOR TO ADDRESS PRIVILEGED USER RESPONSIBILITIES

Cybersecurity Framework Security Function: *Protect*
FY 2023 IG FISMA Reporting Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 5, security control PL-4, Rules of Behavior (ROB), states the following:

> Control:
> a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
> b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

NIST further clarifies that organizations should consider the ROB based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

[9] Ibid 7.

USADF did not establish a ROB that describes privileged users' responsibilities and expected behavior for information and system usage, security, and privacy. The ROB only required a more complex password for privileged users.

USADF management stated that its ROB applies to all users, including network administrators, system administrators, designers, developers, employees, contractors, and end-users. USADF management also indicated that only three personnel were privileged users and they have not had turnover in those positions for several years. Due to these factors, USADF did not believe there was a need to create a separate ROB for its privileged users.

A privileged user has elevated access privileges, such as administrator rights and access to critical system files and data. Therefore, it is important to continually remind privileged users of their responsibilities and terms of use for these accounts. Improperly used privileged accounts increases the risk of compromised USADF systems leading to unauthorized access to the organization's sensitive information.

Upon notification of this issue, USADF management documented its privileged users' responsibilities and expected behavior when accessing agency information systems. In addition, USADF's privileged users signed acknowledgements that they read, understood, and agreed to abide by the ROB. Therefore, we are not making a recommendation.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USADF provided an updated final action date for the prior recommendation associated with Finding 1 in this report. USADF's comments are included in their entirety in Appendix II.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to determine whether USADF implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the current IG FISMA reporting metrics.

Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The scope of this performance audit was to assess USADF's information security program consistent with FISMA and reporting instructions issued by OMB and the Council of the Inspectors General on Integrity and Efficiency. In accordance with those instructions, we assessed 20 core metrics and 20 supplemental metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA Reporting Metrics, for a sample of 3 of 10 internal and external information systems in USADF's FISMA inventory as of October 5, 2022.

In addition, we performed an internal vulnerability assessment of USADF's network. The audit also included a follow up on prior audit recommendations[10] to determine whether USADF made progress in implementing them. See Appendix III for the status of the prior recommendations.

Audit fieldwork was conducted at USADF's headquarters located in Washington, DC, from November 30, 2022, to June 15, 2023. It covered the period from October 1, 2022, through June 15, 2023.

Methodology

To determine if USADF implemented an effective information security program, CLA conducted interviews with USADF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, CLA reviewed documents supporting the information security program. These documents included, but were not limited to, USADF's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management

[10] Recommendations 1 and 3 in *USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-ADF-22-001-C, November 8, 2021).

procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, CLA compared documents, such as USADF's information technology policies and procedures, to requirements stipulated in Executive Order 14028, relevant OMB memorandums, and NIST special publications. CLA also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, CLA reviewed the status of FISMA audit recommendations from fiscal year 2021.[11] See Appendix III for the status of prior year recommendations.

In assessing the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. CLA considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, CLA considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, based on risk, significance, or criticality this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

To perform our audit of USADF's information security program and practices, CLA followed a work plan based on, but not limited to, the following guidance:

- *Government Auditing Standards* (April 2021).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022).
- Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities.*
- FY 2023 IG FISMA Reporting Metrics (February 10, 2023).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* for specification of security controls (December 10, 2020).
- NIST SP 800-53A*,* Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy,* for the risk management framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (February 2014).
- USADF policies and procedures.

[11] Ibid 8.

Appendix II

MANAGEMENT COMMENTS

August 17, 2023

Mr. Alvin Brown
Deputy Assistant Inspector General for Audit
USAID, Officer of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523

Subject: Audit of the United States African Development Foundation (USADF): Response to the Draft Evaluation Report on USADF's Compliance with FISMA for FY 2023 (Report No. A- ADF-23-00X-C)

Dear Mr. Brown:

This letter responds to the findings presented in your above-captioned draft report. We appreciate your staff's efforts in working with us to improve the Foundation's information security program and compliance with the provisions of the Federal Information Security Management Act of 2014 and NIST SP 800-53. We have reviewed your report and have the following comment in response to your recommendation.

Recommendation 1.
We recommend that United States African Development Foundation's Chief Information Security Officer formally document and implement a process for validating that medium and low risk vulnerabilities are remediated in accordance with the agency's policy.

Management Response:

We accept the recommendation that USADF's Chief Information Security Officer formally document and implement a process for validating that medium and low risk vulnerabilities are remediated in accordance with the agency's policy. Final action on this finding and recommendation is to be completed by March 31, 2024.

/s/
Travis Adkins
President and CEO

Cc: Solomon Chi, Chief Information Security Officer
Mathieu Zahui, CFO
Ellen Teel, Senior Auditor

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2021[12] FISMA audit recommendations.

No.	FY 2021 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
1	We recommend that USADF's Chief Information Security Officer formally document and implement a process for validating that medium and low risk vulnerabilities are remediated in accordance with the agency's policy.	Open	Agree. See Finding 1.
3	We recommend that USADF's Chief Financial Officer design and implement a process to screen USADF contractors at the extent and level appropriate to the risks associated with the position.	Closed	Agree

[12] Ibid 8.