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

USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA

Audit Report A-ADF-22-001-C
November 8, 2021

Information Technology Audits Division

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

MEMORANDUM

DATE: November 8, 2021

TO: USADF, Acting President and Chief Executive Officer, Elisabeth Feleke

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

SUBJECT: USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-ADF-22-001-C)

Enclosed is the final audit report on the U.S. African Development Foundation's (USADF) information security program for fiscal year (FY) 2021, in support of the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the audit. The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on 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.[1] To answer the audit objective, CLA evaluated the effectiveness of USADF's implementation of the FY 2021 Inspector General (IG) FISMA Reporting Metrics[2] that fall into the nine domains in the following table. Also, CLA assessed USADF's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." CLA reviewed four of the eleven information systems in USADF's

[1] 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.

[2] Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," May 12, 2021.

inventory dated February 17, 2021. Audit fieldwork covered USADF's headquarters located in Washington, DC, from April 13, 2021, to August 12, 2021. It covered the period from October 1, 2020, through August 12, 2021.

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

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

However, as summarized in the table below, CLA noted four weaknesses in three of the nine FY 2021 IG FISMA metric domains.

Fiscal Year 2021 **IG FISMA Metric Domains**	**Weaknesses** **Identified**
Risk Management	
Supply Chain Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	

To address the weaknesses identified in CLA's report, we recommend that USADF's:

Recommendation 1. Chief Information Security Officer document and implement a process for validating that medium and low risk vulnerabilities are remediated in accordance with the agency's policy.

Recommendation 2. Chief Information Security Officer develop and implement a process to monitor privileged activities, including which activities to monitor as well as the process and frequency for monitoring those activities.

Recommendation 3. 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.

Recommendation 4. Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy & Policy.

In finalizing the report, the audit firm evaluated USADF's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1, 2, 3, and 4 resolved but open pending completion of planned activities. For the four recommendations, please provide evidence of final action to OIGAuditTracking@usaid.gov.

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

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

Fiscal Year 2021

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

November 8, 2021

Ms. Lisa Banks
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Ms. Banks:

CliftonLarsonAllen LLP (CLA) is pleased to present our final report on the results of our audit of the United States African Development Foundation's (USADF) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2021.

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

Very truly yours,

Sarah Mirzakhani, CISA
Principal

Inspector General
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 2021 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 current year IG FISMA reporting metrics.

For this year's review, OMB required IGs to assess 66 metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each function area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The audit included an assessment of USADF's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope also included assessing selected security controls outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 4 of 11 internal and external systems in USADF's FISMA inventory of information systems.

Audit fieldwork covered USADF's headquarters located in Washington, DC, from April 13, 2021, to August 12, 2021. It covered the period from October 1, 2020, through August 12, 2021.

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

We concluded that USADF implemented an effective information security program by achieving an overall *Optimized* maturity level based on the FY 2021 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 four weaknesses that fell in the supply chain risk management, configuration management, and identity and access management domains of the FY 2021 IG FISMA reporting metrics and have made four recommendations to assist USADF in strengthening its information security program.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from USADF on or before November 8, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 8, 2021.

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
November 8, 2021

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[1] (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.[2]

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

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

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

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 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[3] to independently assess their agencies' information security program.

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

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

[3] We submitted our responses to the FY 2021 IG FISMA reporting metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

As highlighted in Table 1, the fiscal year (FY) 2021 IG FISMA reporting metrics are designed to assess the maturity[4] 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. The FY 2021 IG FISMA reporting metrics include a new Supply Chain Risk Management (SCRM) domain within the Identify function area; however, the SCRM domain was not considered in the Identify framework function rating.

For FY 2021, OMB required IGs to assess 66 metrics in the five security function areas to determine the effectiveness of their information security program and the maturity level of each function area.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 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 2021 IG FISMA reporting metrics for a sample of 4 of 11 USADF internal and external information systems[6] in USADF's FISMA inventory as of February 17, 2021.

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.

[4] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized. To be considered effective, an Agency's information security program must be rated *Managed and Measurable* (Level 4).

[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 four sampled information systems since 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.

Audit Results

We concluded that USADF implemented an effective information security program by achieving an overall *Optimized* maturity level based on the FY 2021 IG FISMA reporting metrics.[7] For example, USADF:

- Maintained an enterprise risk management program.
- Implemented an effective security training 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 2021 IG FISMA reporting metrics.

Table 2: Maturity Levels for the FY 2021 IG FISMA Reporting Metrics

Security Function	FY 2021 Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Optimized	**Risk Management**	Optimized
		Supply Chain Risk Management	Ad Hoc[8]
Protect	Managed and Measurable	**Configuration Management**	Managed and Measurable
		Identity and Access Management	Managed and Measurable
		Data Protection and Privacy	Consistently Implemented
		Security Training	Managed and Measurable
Detect	Optimized	**Information Security Continuous Monitoring**	Optimized
Respond	Managed and Measurable	**Incident Response**	Managed and Measurable
Recover	Consistently Implemented	**Contingency Planning**	Consistently Implemented
Overall	**Level 5: Optimized - 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 four weaknesses that fell in the supply chain risk management, configuration management, and identity and access management domains of the FY 2021 IG FISMA Metrics (see Table 3) and have made four recommendations to assist USADF in strengthening its information security program.

[7] In accordance with the FY 2021 IG FISMA reporting metrics, ratings throughout the nine domains were determined by a simple majority, where the most frequent level across the metrics served as the domain rating. Agencies were rated at the higher level in instances when two or more levels were the most frequently rated. The domain ratings inform the overall function ratings, and the five function ratings inform the overall agency rating.

[8] The FY 2021 IG FISMA reporting metrics indicated that, to provide agencies with sufficient time to fully implement NIST Special Publication 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore would not be considered for the overall rating.

Table 3: Weaknesses Noted in the FY 2021 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	None
	Supply Chain Risk Management	USADF Needs to Document Supply Chain Risk Management Procedures (**See Finding # 4**)
Protect	**Configuration Management**	USADF Needs to Continue to Strengthen its Vulnerability and Patch Management Process **(See Finding # 1)**
	Identity and Access Management	USADF Needs to Monitor Privileged User Activities **(See Finding # 2)** USADF Needs to Ensure All Personnel are Appropriately Screened **(See Finding # 3)**
	Data Protection and Privacy	None
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

In addition, USADF took corrective action to close the four open recommendations from the FY 2017[9] and FY 2020[10] FISMA audits. Refer to Appendix III for the status of prior year recommendations.

In response to the draft report, USADF outlined and described its plans to address all four recommendations. Based on our evaluation of management comments, we acknowledge USADF's management decisions on all four recommendations. Further, we consider these recommendations resolved, but open pending completion of planned activities. 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.

[9] *USADF Implemented Controls In Support of FISMA for Fiscal Year 2017, But Improvements Are Needed* (Audit Report No. A-ADF-18-001-C, October 2, 2017).

[10] *USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-ADF-21-003-C, December 21, 2020).

AUDIT FINDINGS

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

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Configuration Management*

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal 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:
>
> - High Risk Vulnerabilities must be addressed within 30 days.
> - Moderate Risk Vulnerabilities must be addressed within 90 days.
> - Low Risk Vulnerabilities must be addressed within 120 days.

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

> i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.
>
> Agencies shall:
> * * *
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

We performed independent vulnerability scans and identified no critical or high-risk vulnerabilities. However, we identified medium and low risk vulnerabilities due to missing patches and configuration weaknesses. Specifically, credentialed scans[11] identified 125 medium and one low risk vulnerability, including vulnerabilities publicly known from 2012 through 2021. Of the 126 medium and low vulnerabilities, 30 medium vulnerabilities were also identified in our independent scans on the same Internet Protocol addresses in the FY 2020 audit.

[11] A credentialed vulnerability scan uses administrative access to the system being scanned that allows for more detailed scanning to identify vulnerabilities that can not to be seen from the network.

In addition, our non-credentialed scans identified 10 medium and 19 low risk vulnerabilities, including vulnerabilities publicly known from 2001 through 2021. Of the 29 medium and low risk vulnerabilities, 16 were also identified in our independent scans on the same IP addresses in the FY 2020 audit.

USADF indicated that, due to resource constraints, they focused resources on remediating critical and high-risk vulnerabilities and remediating medium and low risk vulnerabilities as time permitted. In addition, USADF did not have a process in place for validating that medium and low risk vulnerabilities were remediated in accordance with the timelines defined in the agency's policy.

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. This may expose USADF's systems to unauthorized access, data loss, data manipulation and system unavailability. In addition, delaying remediation of vulnerabilities may increase the risk that an attacker can combine lower risk vulnerabilities with other attacks to increase their exploitation potential. Therefore, we are making the following recommendation.

> ***Recommendation 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.*

2. USADF NEEDS TO MONITOR PRIVILEGED USER ACTIVITIES

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Identity and Access Management*

NIST Special Publication 800-53, Revision 4, security control AU-6, Audit and Accountability, states the following regarding audit review, analysis, and reporting:

> The organization:
>
> a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
> b. Reports findings to [Assignment: organization-defined personnel or roles].

USADF was not reviewing activities of privileged users though certain activities were logged. Management stated there was not a documented process in place for determining the privileged activities to monitor and reviewing those specified user activities.

A privileged user has elevated access privileges, such as administrator rights and access to critical system files and data. Therefore, it is important to monitor privileged user activities to make sure those privileges are not misused or compromised. Without monitoring privileged user activities, detection and response to a data breach may be impacted and unauthorized system changes may occur without management's knowledge. Therefore, we are making the following recommendation.

> ***Recommendation 2:*** *We recommend that USADF's Chief Information Security Officer develop and implement a process to monitor privileged activities, including which activities to monitor as well as the process and frequency for monitoring those activities.*

3. USADF NEEDS TO ENSURE ALL PERSONNEL ARE APPROPRIATELY SCREENED

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Identity and Access Management*

NIST Special Publication 800-53, Revision 4, security control PS-3, Personnel Security, states the following regarding personnel screening:

> The organization:
>
> a. Screens individuals prior to authorizing access to the information system.

Additionally, the *USADF IT Security Implementation Handbook*, section 6, states, "All individuals, requiring access to USADF information and information systems, must be screened before their access authorization has been granted."

USADF did not ensure that all personnel were appropriately screened prior to being granted system access. Specifically, USADF did not screen 12 of 13 contractors. Of the 12 contractors, 2 had privileged access and 1 had access to sensitive information system security documentation.

Management stated that USADF's information is controlled but unclassified and that background requirements in accordance with USADF's classification fall under non-sensitive positions for government. In view of this sensitivity of information, USADF management decided that contractors, consultants, or personal service contractors were not required to undergo background investigations during their hiring process unless the Department of Interior, which is responsible for personnel background screening, determined the need for it. Management also stated that, as required by respective contracts, its contractors, personal service contractors, and consultants must sign a non-disclosure agreement upon hiring. In addition, management indicated that risk related to access to USADF information systems was mitigated by requiring them to be authenticated by a multi-factor authentication identity access management system, acknowledging the Rules of Behavior, and specialized training.

The purpose of performing background checks is to ascertain the suitability of an individual for a specific position. The depth of background checks should be conducted at the extent and level appropriate to the risks associated with the position. Without sufficient screening of personnel, USADF cannot validate whether individuals are suitable for the level of system access or job responsibilities assigned to them. This is especially important for privileged users and individuals with access to sensitive information system security documentation. The lack of proper screening of USADF personnel can ultimately affect the confidentiality of USADF data. Therefore, we are making the following recommendation.

Recommendation 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.*

4. USADF NEEDS TO DOCUMENT SUPPLY CHAIN RISK MANAGEMENT PROCEDURES

Cybersecurity Framework Security Function: *Identify*
FY 2021 FISMA IG Metric Domain: *Supply Chain Risk Management*

Public law 115-390 – 115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* or the ''SECURE Technology Act" (December 21, 2018) requires executive agencies to develop an overall SCRM strategy and implementation plan and policies and processes to guide and govern SCRM activities.

However, USADF did not document SCRM procedures for processes that USADF is responsible for as discussed in the *USADF Supply Chain Risk Management Strategy & Policy*.

Management stated that the SCRM function is fully outsourced to the Department of Treasury, Bureau of Fiscal Services. Therefore, they did not document SCRM procedures. However, there are certain processes that USADF has responsibility for implementing. For example, USADF specific processes include reporting to the Cybersecurity and Infrastructure Security Agency counterfeit system components when detected, and inspection of laptops when individuals return from travel to high-risk locations.

Without the development of SCRM procedures, certain SCRM processes may not be fully implemented. This may hinder USADF's ability to identify and mitigate supply chain risks. Therefore, we are making the following recommendation.

Recommendation 4: *We recommend that USADF's Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy & Policy.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USADF outlined its plans to address all four recommendations. USADF's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge USADF's management decisions on all four recommendations. Further, we consider these recommendations resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

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 audit was designed 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.

For this year's review, IG's were required to assess 66 metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each function area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The scope of this performance audit was to assess USADF's information security program consistent with FISMA and reporting instructions issued by OMB and DHS. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 4 of 11 internal and external information systems[12] in USADF's FISMA inventory as of February 17, 2021.

In addition, we performed an internal vulnerability assessment of USADF's network. The audit also included a follow up on prior audit recommendations (2017[13] and 2020[14]) to determine whether USADF made progress in implementing them. See Appendix III for the status of the prior recommendations.

Audit fieldwork covered USADF's headquarters located in Washington, DC, from April 13, 2021, to August 12, 2021. It covered the period from October 1, 2020, through August 12, 2021.

Methodology

To determine if USADF implemented an effective information security program, we conducted interviews with USADF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we 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

[12] Ibid 6.

[13] Ibid 9.

[14] Ibid 10.

policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, we compared documents, such as USADF's information technology policies and procedures, to requirements stipulated in NIST special publications. We also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, we reviewed the status of FISMA audit recommendations from fiscal year 2017 and 2020.[15]

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we 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, this resulted in selecting the entire population. However, in cases where entire audit population was not selected, the results cannot be projected and if projected may be misleading.

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

- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements.*
- OMB and DHS, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- NIST Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[15] Ibid 9, and 10.

MANAGEMENT COMMENTS

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

October 5, 2021

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 Audit Report on USADF's Compliance with FISMA for FY 2021 (Report No. A-ADF-22-00X-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 comments in response to your recommendations.

Recommendation No. 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.

> 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. Corrective action will be taken by March 31, 2022.

Recommendation No. 2: We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a process to monitor privileged activities, including which activities to monitor as well as the process and frequency for monitoring those activities.

> We accept the recommendation that USADF's Chief Information Security Officer develop and implement a process to monitor privileged activities, including which activities to monitor as well as the process and frequency for monitoring those activities. Corrective action for documenting and implementing monitoring activities and process will be taken by January 31, 2022.

Recommendation No. 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 risk associated with the position.

> We accept the recommendation that USADF's Chief Financial Officer design and implement a process to screen USADF contractors at the extent and level appropriate to risk associated with the position. Corrective action will be taken by November 30, 2021.

Recommendation No. 4: We recommend that USADF's Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy and Policy.

> We accept the recommendation that USADF's Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy and Policy. USADF will proceed to develop and disseminate Supply Chain Risk Management (SCRM) procedures to its existing SCRM strategy and policy document. Corrective action will be taken by February 28, 2022.

/s/

Elisabeth Feleke
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 2017 and FY 2020[16] FISMA audit recommendations.

No.	FY 2017 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
2	We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to track and remediate vulnerabilities timely in accordance with the foundation's policy. This includes ascertaining that patches are applied timely and are tested prior to implementation into production in accordance with policy.	Closed	Agree

No.	FY 2020 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
1	We recommend that USADF's Chief Information Security Officer should formally document and implement scan configuration reviews to analyze, detect and remediate vulnerabilities.	Closed	Agree
2	We recommend that USADF's Chief Information Security Officer document and implement a process to verify USADF's Authorizing Officials review the authorization packages from the provider organizations as a fundamental basis for determining risk and issue the respective Authorizations to Use for the USADF external systems and/or services.	Closed	Agree
3	We recommend that USADF's Chief Information Security Officer design and implement a process, such as a periodic reconciliation of access agreements on file with a listing of new hires, to validate that all new information system users complete the USADF system access agreements.	Closed	Agree

[16] Ibid 9, and 10.