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

USADF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019

AUDIT REPORT A-ADF-20-002-C
DECEMBER 19, 2019

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, Millennium Challenge Corporation, U.S. African Development Foundation, Inter-American Foundation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: December 19, 2019

TO: USADF, President and Chief Executive Officer, C.D. Glin

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

SUBJECT: USADF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019 (A-ADF-20-002-C)

Enclosed is the final audit report on the U.S. African Development Foundation's (USADF's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2019. 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, the audit firm tested USADF's implementation of selected management, technical, and operational 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 auditors reviewed six of nine information systems in USADF's systems inventory as of February 2019. Fieldwork took place at USADF's headquarters in Washington, DC, from June 6 to

[1] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

October 3, 2019. The audit covered the period from October 1, 2018, through September 25, 2019.

The audit firm concluded that USADF generally implemented an effective information security program by implementing 80 of 85 selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of its information and information systems. Among the controls USADF implemented were the following:

- A security awareness and role-based training program.
- A program for incident handling and response.
- Multifactor authentication for network access to privileged accounts.
- A process to maintain an inventory of information system components.

However, as summarized in the table below, CLA noted weaknesses in two of the eight FISMA metric domains. The weakness occurred because USADF did not implement five controls related to implementing compensating controls and documenting risk acceptances for configuration-related weaknesses. In addition, USADF did not maintain adequate documentation for its user account reviews. With these weaknesses, USADF's information and information systems are potentially exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2019 IG FISMA Metric Domains[2]	**Weaknesses Identified**
Risk Management	
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	

The weakness related to the documentation of user account reviews was raised in previous years. Since a recommendation to address the issue was made previously and has not been

[2] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 9, 2019.

closed, we are not repeating it in this report. To address the other weaknesses identified in the report, we recommend that USADF's chief information security officer:

Recommendation 1: Document and implement compensating controls and acceptance of the risk for information system components when support for the components is no longer available from the developer, vendor, or manufacturer when replacing system components is not feasible.

In finalizing the report, CLA evaluated USADF's response to recommendation 1. After reviewing that evaluation, we consider recommendation 1 resolved, but open pending completion of planned activities. For recommendation 1, please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance extended to our staff and CLA's employees during the engagement.

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

Fiscal Year 2019

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

December 10, 2019

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, D.C. 20005-2221

Dear Mr. Norman:

CliftonLarsonAllen LLP (CLA) is pleased to present our 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 2019.

We appreciate the assistance we received from the staff of USADF and appreciate the opportunity to serve you. 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

CliftonLarsonAllen LLP
CLAconnect.com

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 2019 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether USADF implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls from 6 of 9 of USADF's internal and external information systems. Audit fieldwork was performed at USADF's headquarters in Washington, D.C., from June 6, 2019 to October 3, 2019.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We concluded that USADF generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. Although USADF generally implemented an effective information security program, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in 2 of the 8 Inspector General FISMA Metric Domains and have made one new recommendation 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 current status. We concluded our fieldwork and assessment on October 3, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 3, 2019.

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 USAID Office of Inspector General.

CliftonLarsonAllen LLP

Arlington, Virginia
December 10, 2019

TABLE OF CONTENTS

Summary of Results.....1

Audit Findings.....4

USADF Needs to Strengthen its Vulnerability and Patch Management Process.....4

USADF Needs to Strengthen Its User Account Review Process.....6

Evaluation of Management Comments.....8

Appendix I – Scope and Methodology.....9

Appendix II – Management Comments.....11

Appendix III – Summary of Controls Tested.....13

Appendix IV – Status of Prior Year Findings.....15

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[2] information security program.

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 October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 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 programs.

[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 implementing certain security controls for selected information systems in support of FISMA.

[3] CLA submitted its responses to the FY 2019 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2019, IG FISMA Reporting Metrics are designed to assess the maturity[4] of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Reporting Metric Domains
Identify	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, CLA reviewed selected[5] controls related to the IG FISMA Reporting Metrics from 6 of 9 information systems[6] in USADF's FISMA inventory as of February 2019.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

Audit Results

CLA concluded that USADF generally implemented an effective information security program by implementing 80 of 85[7] selected security controls for selected information systems. For example, USADF:

- Implemented an effective security awareness and role-based training program.
- Maintained an effective program for incident handling and response.
- Implemented multi-factor authentication for network access to privileged accounts.

[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] See Appendix III for a list of controls selected.

[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.

[7] There were 67 unique NIST SP 800-53, Revision 4, controls specifically identified in the FY 2019 IG metrics. We tested the 65 controls that were applicable to systems within the scope of our audit. We also tested 2 additional privacy controls from Appendix J of NIST SP 800-53, Revision 4, because they related to the metrics. A control was counted for each system it was tested against. Thus, there were 85 instances of testing a control.

- Implemented a process to maintain an inventory of information system components.

Although USADF generally implemented an effective information security program, its implementation of 5 of the 85 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. As a result, CLA noted weaknesses in the following IG FISMA Metric Domains (Table 2) and made one recommendation to assist USADF in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2019 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Identify	**Risk Management**	No weaknesses noted.
Protect	**Configuration Management**	USADF Needs to Strengthen its Vulnerability and Patch Management Process **(See Finding # 1)**
	Identity and Access Management	USADF Needs To Strengthen Its User Account Review Process **(See Finding # 2)**
	Data Protection and Privacy	No weaknesses noted.
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	No weaknesses noted.

In response to the draft report, USADF outlined and described its plans to address the one recommendation. Based on our evaluation of management comments, we acknowledge USADF's management decision on recommendation 1. We consider recommendation 1 resolved but open pending completion of planned activities. USADF 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.

AUDIT FINDINGS

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

Cybersecurity Framework Security Function: *Protect*
FY 19 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, states the following regarding flaw remediation:

The organization:

* * *

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

USADF's *Information Technology Department Patch Management Procedures* requires "all patches for vendor maintained systems/applications that are labeled as high/critical and apply to security must also be patched within 90 days of the approved release from the vendor. Any functional but non-critical patches may be installed on a case-by-case basis. USADF IT is responsible for maintaining knowledge of these patches and ensuring that vendors comply with our internal policy."

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states:

i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.

Agencies shall:
* * *

8. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement.
9. Implement and maintain current updates and patches for all software and firmware components of information systems.

NIST Special Publication 800-53, Revision 4, states the following regarding the compensating controls:

Selecting Compensating Security Controls:

Organizations may find it necessary on occasion to employ compensating security controls. Compensating controls are alternative security controls employed by organizations. Compensating controls may be employed by organizations under the following conditions:

- Select compensating controls…if appropriate compensating controls are not available, organizations adopt suitable compensating controls from other sources;
- Provide supporting rationale for how compensating controls provide equivalent security capabilities for organizational information systems and why the baseline security controls could not be employed; and
- Assess and accept the risk associated with implementing compensating controls in organizational information systems.

CLA performed independent vulnerability scans and identified unpatched software, unsupported software, and improper configuration settings which exposed one system to critical and high severity vulnerabilities. The majority of critical and high vulnerabilities were related to missing patches and configuration weaknesses. Specifically, hosts were missing patches that were released for Oracle Java and Microsoft Visual Studio. In addition, Registry configuration weaknesses allowed applied Microsoft patches to not be effective.

Management stated that the vast majority of these vulnerabilities relate to a system that the Department of Treasury utilizes that requires customers (USADF) to use an outdated version of the software. Management documented a risk acceptance memo for the existence of this risk.

It was also noted that one issue related to the registry configuration could not be patched due to a configuration setting restriction on each workstation. However, USADF had not implemented compensating controls or documented its acceptance of that risk. USADF had also not timely patched 45 other identified high/critical vulnerabilities, 37 discovered during credentialed scans[8] and 8 during non-credentialed scans, because it did not have a defined process to track the patching of network devices and servers by the risk-based patch timelines in USADF policies.

Not addressing vulnerabilities in a timely manner may provide sufficient time for attackers to exploit vulnerabilities and gain access to sensitive data potentially exposing USADF's systems to unauthorized access, data loss, data manipulation and system unavailability. Furthermore, unsupported systems are susceptible to old vulnerabilities and exploits that the vendors have addressed with current supported versions.

A recommendation addressing the patch management finding was issued in the FY 2017 FISMA audit.[9] USADF had not yet sufficiently addressed this recommendation through its corrective action and therefore, we are not making a new recommendation at this time.

[8] Credentialed scans were performed utilizing user and/or administrator credentials.

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

However, CLA is making a new recommendation related to implementing compensating controls and documenting risk acceptances for the configuration-related weaknesses.

> ***Recommendation 1:*** *USADF's Chief Information Security Officer should formally document and implement compensating controls and acceptance of the risk for information system components when support for the components is no longer available from the developer, vendor or manufacturer when replacing system components is not feasible.*

2. USADF NEEDS TO STRENGTHEN ITS USER ACCOUNT REVIEW PROCESS

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Identity and Access Management*

NIST Special Publication 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization:
> * * *
> j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].

Additionally, the USADF *Access Control Policy,* states, "An account recertification of USADF users access to IT resources shall be performed annually. USADF IT staff shall request user account recertification from United States (US) Government shared service providers on a yearly basis or agreed upon in the Memorandum of Understanding (MOU) or the Interagency Security Agreement (ISA)."

USADF did not maintain evidence that it performed effective account recertification and/or reviews for five of six sampled systems. Account reviews were initiated and coordinated between USADF and vendor staff, as necessary; however, there are different processes performed for each system. For external systems, the review is initiated and coordinated at the service provider.

While, management has a process to review accounts, as documented in the *Access Control Policy*, it did not have a process in place to maintain adequate evidence to show that account reviews of externally-managed systems were performed, including what accounts were reviewed and what actions were taken as a result of the review.

Without periodically reviewing information system users' account roles and permissions, there is an increased risk that least privilege access may not be maintained and individuals may have more access than is needed to perform their job duties. This could result in users having unauthorized access to sensitive systems and data threatening the confidentiality, integrity, and availability of agency systems.

A recommendation addressing this finding was issued in the FY 2017 FISMA audit.[10] However, USADF had not yet sufficiently addressed this recommendation through its corrective action and therefore, we are not making a new recommendation at this time.

[10] Recommendation 4, *USADF Implemented Controls in Support of FISMA for Fiscal Year 2017* (Audit Report No. A-ADF-18-001-C, October 2, 2017).

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USADF outlined its plan to address recommendation 1. USADF's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge USADF's management decision on recommendation 1. Further, we consider recommendation 1 resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with GAGAS. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit was designed to determine whether USADF implemented an effective[11] information security program.

The audit included tests of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed USADF's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- System Maintenance
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition
- Privacy Controls

For this audit, CLA reviewed selected controls related to the FY2019 IG FISMA Reporting Metrics from 6 of 9 information systems in USADF's systems inventory as of February 2019. See Appendix III for a listing of 67 selected controls.

The audit also included a follow up on prior audit recommendations[12,13] to determine if USADF made progress in implementing the recommended improvements concerning its information security program. See Appendix IV for the status of prior year recommendations.

[11] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[12] *USADF Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-18-001-C, October 2, 2017).

[13] *USADF Has Generally Implemented Controls In Support of FISMA* (Audit Report No. A-ADF-19-002-C, November 2, 2018).

Audit fieldwork was performed at USADF's headquarters in Washington, D.C. from June 6, 2019 to October 3, 2019. It covered the period from October 1, 2018, through September 25, 2019.

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 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 NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. In addition, CLA reviewed the status of FISMA audit recommendations from fiscal year 2017 and 2018.[14]

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. 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 the following guidance:

- OMB and DHS, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular Number A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[14] Ibid 12 and 13.

MANAGEMENT COMMENTS

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

November 26, 2019

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 2019 (Report No. A-ADF-20-00X-C)

Dear Mr. Brown:

This letter responds to the findings presented in your above-captioned draft report. We appreciate your staff 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 the United States African Development Foundation's Chief Information Security Officer should formally document and implement compensating controls and acceptance of the risk for information system components when support for the components is no longer available from the developer, vendor or manufacturer when replacing system components is not feasible.

> We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer should formally document and implement compensating controls and acceptance of the risk for information system components when support for the components is no longer available from the developer, vendor or manufacturer when replacing system components is not

feasible. Final action on this finding and recommendation will be completed by December 10, 2019.

/s/
C.D. Glin
President and CEO

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

SUMMARY OF CONTROLS TESTED

The following table identifies the controls selected for testing.

Control	Control Name	Number of systems tested
AC-1	Access Control Policy and Procedures	1
AC-2	Account Management	6
AC-8	System Use Notification	1
AC-17	Remote Access	1
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	1
AR-4	Privacy Monitoring and Auditing	1
AR-5	Privacy Awareness Training	1
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	6
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	2
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policies and Procedures	1
CM-2	Baseline Configuration	1
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	1
CM-9	Configuration Management Plan	1
CM-10	Software Usage Restrictions	1
CP-1	Contingency Planning Policy and Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing	1
CP-6	Alternate Storage Site	1
CP-7	Alternate Processing Site	1
CP-8	Telecommunication Services	1
CP-9	Information System Backup	1
IA-1	Identification and Authentication Policy and Procedures	1
IR-1	Incident Response Policies and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
IR-7	Incident Response Assistance	1
MP-3	Media Marking	1

Control	Control Name	Number of systems tested
MP-6	Media Sanitization	1
PL-2	System Security Plan	1
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PM-11	Mission/Business Process Definition	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	2
SI-2	Flaw Remediation	1
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-7	Software, Firmware, and Information Integrity	1
SA-3	System Development Life Cycle	2
SA-4	Acquisition Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	6
SA-12	Supply Chain Protection	1
SC-8	Transmission Confidentiality and Integrity	1
SC-28	Protection of Information at Rest	1
SE-2	Privacy Incident Response	1

STATUS OF PRIOR YEAR FINDINGS

The following tables provide the status of the FY 2017[15] and FY 2018[16] FISMA audit recommendations.

No.	FY 2017 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
1	We recommend that the United States African Development Foundation's Chief Information Security Officer strengthen the organization-wide information security program in accordance with National Institute of Standards and Technology standards by developing and implementing documented processes to: a. Develop, communicate and implement an organization wide risk management strategy with the operation and use of the foundation's information systems in accordance with National Institute of Standards and Technology standards. b. Review and update the system security plans to reflect National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. At a minimum, this should include a determination whether the security requirements and controls for the system are adequately documented and reflect the current information system environment. c. Perform information system security assessments on an annual basis in accordance with foundation's policy. d. Review and update the system risk assessments to account for all known vulnerabilities, threat sources, and security controls planned or in place, and determine the resulting level of residual risk to ensure the authorizing official has appropriate knowledge of the security state of the information system. e. Include all known security weaknesses, estimated completion dates and associated corrective plans in the plan of action and milestones and substantiate recommendations are effectively remediated prior to closing them.	Closed	Agree
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	Closed	Disagree, Refer to Finding 1

[15] *USADF Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-18-001-C, October 2, 2017).

[16] *USADF Has Generally Implemented Controls In Support of FISMA* (Audit Report No. A-ADF-19-002-C, November 2, 2018).

No.	FY 2017 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
	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.		
4	We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to enforce the immediate disabling of employee user accounts upon separation from the organization and perform account recertification in accordance with USADF policy, including adhering to the required frequency for recertifying accounts and providing responses.	Closed	Disagree, Refer to Finding 2

No.	FY 2018 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
1	We recommend that the United States African Development Foundation's Chief Information Security Officer fully develop and document a risk management strategy for information technology operations that requires the Foundation to identify: (i) risk assumption; (ii) risk constraints; (iii) risk tolerance; and (iv) priorities and trade-offs.	Closed	Agree
2	We recommend that the United States African Development Foundation's Chief Information Security Officer update the Foundation's access control policies and procedures to include the use of Personal Identity Verification credentials and how the credentials are enforced for logical access to USADF's information technology resources.	Closed	Agree
3	We recommend that the United States African Development Foundation's Chief Information Security Officer update the Foundation's continuous monitoring policies and procedures to include how its Chief Information Officer, Information Technology Systems Administrator, and Security Analyst gather, document, assess, and remediate information system vulnerabilities, threats, and risks in a timely manner and then implement the procedures.	Closed	Agree