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

USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA

AUDIT REPORT A-ADF-21-003-C
DECEMBER 21, 2020

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, and Inter-American Foundation.

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 21, 2020

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

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

SUBJECT: USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA (A-ADF-21-003-C)

Enclosed is the final audit report on the U.S. African Development Foundation's (USADF) information security program for fiscal year 2020 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 tested 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 auditors reviewed three of the nine information systems in USADF's inventory dated May 2020. Fieldwork covered USADF's headquarters in Washington, DC, from May 8 to August 31, 2020. It covered the period from October 1, 2019, through August 31, 2020.

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

The audit firm concluded that USADF generally implemented an effective information security program by implementing 72 of 76[2] instances of selected security controls for selected information systems. Among those controls, USADF:

- Maintained an effective program for enterprise risk management.
- Maintained an effective security awareness training program.
- Maintained an effective inventory management program.
- Implemented an effective program for performing annual system user account reviews.

However, as summarized in the table below, CLA noted weaknesses in three of the eight FISMA metric domains.

Fiscal Year 2020 **IG FISMA Metric Domains**[3]	**Weaknesses Identified**
Risk Management	
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	X
Incident Response	
Contingency Planning	

To address the weaknesses identified in CLA's report, we recommend that USADF's Chief Information Security Officer take the following actions:

Recommendation 1: Document and implement scan configuration reviews to analyze, detect and remediate vulnerabilities.

Recommendation 2: Document and implement a process to verify USADF's Authorizing Officials review the authorization packages from provider organizations as a fundamental basis for determining risk and issue the respective Authorizations to Use for USADF's external systems and/or services.

[2] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the fiscal year 2020 IG metrics. CLA tested 67 controls. A control was counted for each system it was tested against. Thus, there were 76 instances of testing a control.

[3] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," (April 17, 2020).

Recommendation 3: 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 USADF system access agreements.

In addition, USADF has not taken final corrective action on a recommendation made in our 2017 FISMA audit report[4] regarding a weakness in the Configuration Management domain. See Appendix IV on page 16 of CLA's report for the full text of the recommendation.

In finalizing the report, the audit firm evaluated USADF's responses to the recommendations. After reviewing that evaluation, we consider recommendation 1 resolved but open pending OIG's verification of the agency's final actions and recommendations 2 and 3 resolved but open pending completion of planned activities. 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.

[4] Recommendation 2 in USAID OIG, "USADF Implemented Controls in Support of FISMA for Fiscal Year 2017, But Improvements Are Needed" (A-ADF-18-001-C), October 2, 2017.

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

Fiscal Year 2020

Final Report

CliftonLarsonAllen LLP
CLAconnect.com

December 3, 2020

Mr. Mark Norman
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 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 2020.

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 2020 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 3 of 9 of USADF's internal and external information systems. For this year's review, IGs were also required to assess information security programs on a maturity scale from Level 1 (Ad Hoc) to Level 5 (Optimized) in eight IG FISMA Metric Domains and five Function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and the maturity level of each function area.

Audit fieldwork covered USADF's headquarters located in Washington, DC, from May 8, 2020 to August 31, 2020. It covered the period from October 1, 2019, through August 31, 2020.

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 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 3 of the 8 Inspector General FISMA Metric Domains and have made three new recommendations to assist USADF in strengthening its information security program. In addition, we noted that one recommendation related to a prior year FISMA audit was still open.

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 December 3, 2020. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to December 3, 2020.

A member of
Nexia
International

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
December 3, 2020

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[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 November 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 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 2020 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2020 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, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2020 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2020 IG FISMA 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 for 3 of 9 information systems[6] in USADF's FISMA inventory as of May 2020.

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 72 of 76[7] selected security controls for selected information systems. For example, USADF:

- Maintained an effective program for enterprise risk management;
- Maintained an effective security awareness training program;
- Maintained an effective inventory management program; and
- Implemented an effective program for performing annual system user account reviews.

[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.

[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 86 NIST SP 800-53, Revision 4, controls, including enhancements specifically identified in the FY 2020 IG metrics. We tested 67 controls. A control was counted for each system it was tested against. Thus, there were 76 instances of testing a control. See Appendix III for a list of the controls.

Although USADF generally implemented an effective information security program, its implementation of 4 of the 76 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 three recommendations to assist USADF in strengthening its information security program. In addition, we noted that one recommendation related to a prior year FISMA audit is still open.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2020 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Metric Domains	Weaknesses Noted in FY 2020
Identify	**Risk Management**	None
Protect	**Configuration Management**	USADF Needs to Strengthen its Vulnerability and Patch Management Process **(See Finding # 1)**
	Identity and Access Management	USADF Needs To Ensure All Information System Users Complete Access Agreements **(See Finding # 3)**
	Data Protection and Privacy	None
	Security Training	None
Detect	**Information Security Continuous Monitoring**	USADF Needs To Maintain Its Security Authorization Process in Accordance with NIST requirements. **(See Finding # 2)**
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

In response to the draft report, USADF outlined and described its plans to address all three recommendations. Based on our evaluation of management comments, we acknowledge USADF's management decisions on all three recommendations. Further, we consider these recommendations 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, Appendix II includes USADF management comments, Appendix III identifies the controls selected for testing, and Appendix IV provides the status of prior year recommendations.

AUDIT FINDINGS

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

Cybersecurity Framework Security Function: *Protect*
FY 2020 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:

* * *

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.

USADF's *Information Technology Department Patch Management Procedures* states, "All high/critical patches must be applied as soon as practically possible, but not longer than 30 calendar days after public release for any critical production server. All patches that are medium/high severity or for non-critical systems must be rolled out within 90 calendar days."

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.

CLA performed independent vulnerability scans and identified unpatched software and improper configuration settings which exposed five hosts to critical and high severity vulnerabilities. The majority of critical and high vulnerabilities were related to missing patches and configuration weaknesses. Specifically, one host was missing cumulative Microsoft operating system and Adobe patches since 2019; two hosts were missing patches that were released for Oracle Java and two hosts had default Simple Network Management Protocol (SNMP) names.

USADF indicated they had not timely patched the identified critical and high vulnerabilities because their Nessus[8] scan configuration setting was not configured to scan for all vulnerabilities. Specifically, USADF had not reviewed the configuration of its scans and used the default scan policies for Nessus. Management stated they are proceeding with remediation of the affected hosts.

The FY 2017 FISMA audit report[9] made a recommendation to track and remediate vulnerabilities timely in accordance with the foundation's policy, including ensuring that patches are applied timely. Based on the results of our independent scans indicating missing patches, we noted this recommendation remains open.

Management stated that the identified Java vulnerabilities related to the same system with an outdated version of the software as last year that the Department of Treasury requires customers (USADF) to use. To address this issue, the FY 2019 FISMA audit[10] made a recommendation to 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. USADF documented a risk acceptance memo dated January 31, 2020 to address vendor unsupported software; however, it expired July 31, 2020. Upon notification of the expired risk acceptance to management, the Authorizing Official (AO) signed a new risk acceptance memo with compensating controls, covering a period of three years that will expire upon the expiration date of the system authorization to operate. Therefore, we consider the prior year recommendation closed.

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. Without the proper Nessus scan configuration, certain vulnerabilities may go undetected.

In addition to the FY 2017 FISMA recommendation that remains open, we are making a new recommendation to address the configuration of USADF's scanning tool.

> ***Recommendation 1:*** *USADF's Chief Information Security Officer should formally document and implement scan configuration reviews to analyze, detect and remediate vulnerabilities.*

[8] Nessus is a vulnerability scanner developed by Tenable, Inc.

[9] Recommendation 2, *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] Recommendation 1, *USADF Has Generally Implemented Controls In Support of FISMA* (Audit Report No. A-ADF-20-002-C, December 19, 2019).

2. USADF NEEDS TO MAINTAIN ITS SECURITY AUTHORIZATION PROCESS IN ACCORDANCE WITH NIST REQUIREMENTS

Cybersecurity Framework Security Function: *Detect*
FY 20 FISMA IG Metric Domain: *Information Security Continuous Monitoring*

NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privac*y, states the following regarding the security authorization process:

- An Authorization to Use (ATU) is used when an organization chooses to accept the information in an existing authorization package produced by another organization (either federal or nonfederal) for an information system that is authorized to operate by a federal entity. An authorization to use is issued by an authorizing official from the customer organization instead of an authorization to operate.
- An authorization to use requires the customer organization to review the authorization package from the provider organization as the fundamental basis for determining risk.
- Once the customer organization is satisfied with the security and privacy posture of the shared or cloud system, application, or service (as reflected in the current authorization package) and the risk of using the shared or cloud system, application, or service has been sufficiently mitigated, the customer organization issues an authorization to use in which the customer organization explicitly understands and accepts the security or privacy risk incurred by using the shared system, service, or application.

USADF did not maintain its security authorization process in accordance with NIST requirements for nine[11] external systems and/or services. Three systems are managed by Federal Risk and Authorization Management Program (FedRAMP)[12] cloud service providers and six systems are managed by two federal shared service providers. Specifically, the AO did not review the authorization package from the provider organization, and formally document an explicit understanding and acceptance the security or privacy risk incurred by using the external system or service.

The USADF Chief Information Security Officer (CISO) documented a risk acceptance memo for each external system and/or service to the AO in January/February 2020; however, the AO did not issue an ATU until CLA brought the requirement to management's attention during the FISMA audit fieldwork in May 2020.

In addition, prior to issuing the ATUs, USADF did not review the authorization package from the provider organization as the fundamental basis for determining risk for the external systems as required by NIST. Instead, management reviewed Service Organization Control Reports, Inter Agency Agreements, and Service Level Agreements as the basis for understanding and accepting the security and privacy risk incurred by the USADF for using these federal shared systems and services, and FedRAMP systems.

[11] Only two of these systems were included in the audit scope, however management provided risk assessments for all nine systems, and the issue was noted upon our review of the risk assessments.

[12] FedRAMP is a government-wide program for cloud products and services that provides a standard approach to security assessment, authorization, and continuous monitoring activities.

Management stated they were unaware of the NIST requirement for the AO to issue an ATU for an external system or service that USADF uses. Management indicated that they believed the risk assessments performed by the CISO were sufficient to document the risk incurred by USADF for using the external systems and services.

Without the AO reviewing the authorization package for the external systems and services, and authorizing the systems and services to use, USADF did not ensure that an appropriate senior official was accountable for explicitly understanding and accepting the security or privacy risk incurred by using the external system or service. To assist USADF in properly authorizing the external systems and services in accordance with NIST we made the following recommendation.

> ***Recommendation 2:*** *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.*

3. USADF NEEDS TO ENSURE ALL INFORMATION SYSTEM USERS COMPLETE ACCESS AGREEMENTS

Cybersecurity Framework Security Function: *Protect*
FY 20 FISMA IG Metric Domain: *Identity and Access Management*

NIST Special Publication 800-53, Revision 4, security control PS-6, states the following regarding access agreements:

> The organization:
> * * *
> c. Ensures that individuals requiring access to organizational information and information systems:
>   1. Sign appropriate access agreements prior to being granted access.

Additionally, the *USADF IT Security Implementation Handbook*, s*ection 5.8.6 – Access Agreements (PS-6),* states, "All USADF personnel receive and sign the USADF Computer System Access Agreement and USADF IT Security Awareness Contract during initial security awareness training."

USADF did not ensure all network users completed system access agreements (Rules of Behavior) prior to gaining system access. Specifically, we noted that two out of the total population of eight newly hired employees did not complete a signed access agreement, in accordance with NIST requirements and USADF policy. These employees onboarded to USADF in April of 2020. Upon notification of the issue to management, the CISO required the employees to sign the access agreements electronically.

Management stated that new hires sign access agreements in hard copy format on the day they onboard to USADF prior to gaining a laptop or workstation and system access. Due to the COVID-19 pandemic this year, new hires were onboarded without going to the USADF office, therefore the access agreements for the two sampled new hires were not signed. The CISO stated that due to an oversight, follow up was not conducted to ensure the forms were signed electronically as soon as the users gained system access.

Without ensuring new information system users complete access agreements prior to gaining system access, there is increased risk that system users do not understand their responsibilities when accessing the USADF's information systems and managing the organization's data. Requiring the completion of the access agreement ensures that users read, understand, and agree to follow the rules and limitations related to the systems that they are authorized to access. To assist USADF in strengthening personnel security controls related to accessing information systems we made the following recommendation.

> ***Recommendation 3:*** *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.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USADF outlined its plans to address all three 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 three recommendations. Further, we consider these recommendations 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 objective. The audit was designed to determine whether USADF implemented an effective[13] 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 FY2020 IG FISMA Reporting Metrics from 3 of 9 information systems in USADF's systems inventory as of May 2020. In addition, we performed a vulnerability assessment of the USADF local area network. See Appendix III for a listing of the selected controls.

The audit also included a follow up on prior audit recommendations[14] [15] (2017 and 2019) 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.

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

[14] *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).

[15] *USADF Has Generally Implemented Controls In Support of FISMA* (Audit Report No. A-ADF-20-002-C, December 19, 2019).

Audit fieldwork covered USADF's headquarters located in Washington, DC, from May 8, 2020 to August 31, 2020. It covered the period from October 1, 2019, through August 31, 2020.

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 2019.[16]

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 2020 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 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[16] Ibid 14, and 15.

MANAGEMENT COMMENTS

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

November 19, 2020

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 2020 (Report No. A-ADF-21-00X-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 the United States African Development Foundation's Chief Information Security Officer should formally document and implement scan configuration reviews to analyze, detect and remediate vulnerabilities.

> We accept the recommendation that USADF's Information Security Officer formally document and implement scan configuration reviews to analyze, detect and remediate vulnerabilities. Final action on this finding and recommendation will be completed by November 30, 2020.

Recommendation No. 2: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to ensure USADF's Authorizing Officials (AO) 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.

> We accept the recommendation that USADF's Chief Information Security Officer document and implement a process to ensure USADF's Authorizing Officials (AO) 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. Due to COVID-19, external systems cannot provide review of their authorization packages through established reading rooms or other prior alternative methods. USADF is working with external system owners and providers to determine availability to review their authorization packages as a basis for determining risk, and to issue Authorization to Use for the USADF external systems and/or services. Corrective Action is to be completed by September 15, 2021.

Recommendation No. 3: We recommend that the United States African Development Foundation'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.

> We accept the recommendation 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. Corrective action is expected to be completed by December 15, 2020.

/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	3
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	3
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	1
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	3
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
MP-6	Media Sanitization	1

Control	Control Name	Number of systems tested
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	3
SA-3	System Development Life Cycle	1
SA-4	Acquisition Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	2
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
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
	Total Control Instances Tested	**76**

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2017 and FY 2019[17] 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	Disagree, Refer to Finding 1
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	Agree

No.	FY 2019 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 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.	Closed	Agree

[17] Ibid 14, and 15.