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

USADF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018

AUDIT REPORT A-ADF-19-002-C
NOVEMBER 2, 2018

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

Office of Inspector General, U.S. Agency for International Development

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, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, 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: November 2, 2018

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 2018 (A-ADF-19-002-C)

Enclosed is the final audit report on the U.S. African Development Foundation's (USADF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2018. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown and Company CPAs and Management Consultants PLLC (Brown) to conduct the audit. The contract required Brown to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Brown'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. Brown is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Brown did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USADF implemented selected security controls for certain information systems in support of FISMA. To answer the audit objective, Brown evaluated USADF's implementation of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Brown reviewed selected controls for USADF's internal system and six external systems. The firm also performed a vulnerability assessment of USADF's internal system and an evaluation of USADF's process for identifying, correcting, and mitigating technical vulnerabilities. Fieldwork was performed at USADF's headquarters in Washington, DC, from April 16 through September 7, 2018.

The audit firm concluded that USADF generally complied with FISMA by implementing 46 of 59 security controls reviewed for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems. Among the controls USADF implemented were the following:

- Developed and partially implemented an organization-wide risk management strategy for the operation and use of its internal applications and applications run by shared service providers in accordance with National Institute of Standards and Technology (NIST) guidance.
- Reviewed and updated the system security plan and security assessment and authorization documentation for its internal system in accordance with NIST Special Publication 800-53.
- Performed information system security assessments annually in accordance with USADF's policy.
- Reviewed and updated system risk assessments taking into account vulnerabilities, threats, and security controls planned or in place.
- Developed and fully implemented a documented process to ensure that the plan of action and milestones (POA&M) identified all known security weaknesses, associated corrective plans, and estimated completion dates.
- Developed and implemented a documented process to remediate vulnerabilities timely in accordance with the Foundation's policy.
- Developed and implemented a documented process to migrate unsupported applications to vendor-supported platforms.

However, Brown identified weaknesses. USADF did not implement 13 controls related to risk management, account management, multifactor authentication, and continuous monitoring.

To address the weaknesses identified in the report, we recommend that USADF's chief information security officer:

Recommendation 1. Fully develop and document a risk management strategy for information technology operations that requires the Foundation to identify risk assumptions, risk constraints, risk tolerance, and priorities and trade-offs.

Recommendation 2. 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.

Recommendation 3. 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.

In finalizing the report, Brown evaluated USADF's responses to the recommendations. After reviewing that evaluation, we consider all three recommendations resolved but open pending completion of planned activities.

For recommendations 1 through 3, please provide evidence of final action to OIGAuditTracking@usaid.gov.

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

The U.S. African Development Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018

Final Report

October 22, 2018

Prepared by

Brown & Company CPAs and Management Consultants, PLLC
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Mr. Mark S. 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:

Enclosed is our report on the U.S. African Development Foundation's (USADF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The African Development Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018.* The USAID Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs and Management Consultants, PLLC to conduct the audit in support of the FISMA requirement for an annual evaluation of USADF's information security program.

The objective of this performance audit was to determine whether USADF implemented selected security controls for certain information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

For this audit, we reviewed selected controls from USADF's seven information systems. The audit also included a vulnerability assessment of one internal system and an evaluation of USADF's process for identifying and mitigating information systems vulnerabilities. Audit fieldwork was performed at USADF's headquarters in Washington, D.C., from April 16, 2018 through September 7, 2018.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

The audit concluded that USADF generally complied with FISMA requirements by implementing many selected security controls for selected information systems. Although USADF generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

1101 MERCANTILE LANE, SUITE 122 • LARGO, MD 20774
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@brownco-cpas.com • www.brownco-cpas.com

Consequently, the audit identified areas in USADF's information security program that needed to be improved. We are making three recommendations to assist USADF in strengthening its information security program. In addition, findings related to recommendations from prior years were not yet fully implemented.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of USADF and the opportunity to serve you. We will be pleased to discuss any questions you may have.

Brown & Company CPAs and Management Consultants, PLLC
October 22, 2018
Largo, Maryland

Table of Contents

Summary of Results

The Federal Information Security Modernization Act of 2014 [1] (FISMA), requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems[2], including those provided or managed by another agency, contractor, or other source. Because the United States African Development Foundation (USADF or Foundation) is a federal agency, it is required to comply with federal information security requirements.

FISMA also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capabilities are 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. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for federal agencies.

The U.S. Agency for International Development's (USAID) Office of Inspector General (OIG) engaged us, Brown & Company CPAs and Management Consultants, PLLC, to conduct an audit in support of the FISMA requirement for an annual evaluation of USADF's information security program. The objective of this performance audit was to determine whether USADF implemented selected security controls for certain information systems in support of FISMA.

Our audit was performed 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this audit, we reviewed selected controls from one USADF-managed internal system and six external systems.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283— December 18, 2014) amends the Federal Information Security Management Act of 2002.
[2] 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.

Results

We concluded that USADF generally complied with FISMA by implementing 46 of 59[3] security controls reviewed for selected information systems. For example, USADF did the following:

- Developed and partially implemented an organization-wide risk management strategy for operation and use of its internal and applications run by shared service providers in accordance with National Institute of Standards and Technology guidance.
- Reviewed and updated system security plan and security assessment and authorization documentation in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems*.
- Performed information system security assessments on an annual basis in accordance with USADF's policy.
- Reviewed and updated system risk assessments to account for vulnerabilities, threat sources, and security controls planned or in place.
- Developed and fully implemented a documented process to ensure that plan of action and milestones (POA&Ms) identified all known security weaknesses, associated corrective plans, and estimated completion dates in the POA&Ms, and demonstrated that recommendations were effectively remediated prior to closing them.
- Developed and implemented a documented process to remediate vulnerabilities timely in accordance with the Foundation's policy.
- Developed and implemented a documented process to migrate unsupported applications from their existing platform to platforms that are vendor-supported.

Although USADF generally had policies for its information security program, its implementation of those policies for 13 of 59 security controls reviewed was not fully effective to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in USADF's information security program that needed to be improved. Specifically, USADF needs to:

- Continue strengthening the risk management strategy portion of its organization-wide information security program.
- Strengthen account management controls.
- Fully implement multifactor authentication for non-privileged accounts.
- Document the daily continuous monitoring activities of the Chief Information Security Officer, the Information Technology (IT) Systems Administrator, and the IT Security Analyst.

[3] See Appendix IV for the number of selected controls tested.

As a result, USADF's operations and assets may be at risk of unauthorized access, misuse and disruption. This report makes three recommendations to assist USADF in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to 4 of 17 prior years recommendations had not yet been fully implemented, and therefore, new recommendations were not made. Detailed findings appear in the following section.

Audit Findings

USADF Needs to Continue Strengthening the Risk Management Strategy Portion of its Organization-Wide Information Security Program

FISMA requires agencies to develop, document and implement an agency-wide information security program to provide information security for the information and information systems that support the agency's operations. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that organization-wide information security program management controls place an emphasis on the overall security program and are intended to enable compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

NIST SP 800-53, Revision 4, security control PM-9, Risk Management Strategy, states the following regarding an entity-wide risk management strategy:

> The organization:
>
> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
> b. Implements the risk management strategy consistently across the organization; and
> c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
>
> Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

USADF in recent years has undergone major changes in its information technology (IT) assets and data hosting and processing activities. As part of the management of its systems development life cycle, USADF has adopted and implemented policies and operating procedures that strengthen its actions and likely outcomes in the areas of security and privacy controls implementation. However, USADF has not defined and documented policies and procedures that describe how the Foundation does the following: (i) assess risk; (ii) respond to risk once determined; and (iii) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement.

In Fiscal Year (FY) 2018 USADF developed and implemented security assessment and authorization documents, such as a system security plan, a security assessment report, and plans of action and milestones documents, which are key inputs to an organization-wide risk

management strategy for its IT operations. However, USADF did not fully develop a risk management strategy for the Foundation's IT operations and mission support function that addresses how the Foundation intends to: assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that USADF routinely uses in making both IT investment and operational decisions. The risk management strategy would also establish USADF's basis for managing risk and delineate the boundaries for risk-based decisions within the Foundation.

Without developing, documenting and communicating an organization-wide risk management strategy that includes USADF's IT operations, information technology strategic goals, and objectives, requirements for protecting information and information systems may not be aligned with the risk tolerance that supports USADF's mission and business priorities. Ultimately, this may lead to inconsistently managing and monitoring information security-related risks associated with maintaining the confidentiality, integrity and availability of the Foundation's information.

> **Recommendation 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 assumptions; (ii) risk constraints (iii) risk tolerance; and (iv) priorities and trade-offs.

USADF Needs to Strengthen Account Management Controls

NIST SP 800-53, Revision 4, security control AC-2, Account Management, states the following regarding account management:

> The organization:
>
> …
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].
> g. Monitors the use of information system accounts;
> h. Notifies account managers:
>
> 1. When accounts are no longer required;
> 2. When users are terminated or transferred; and
> 3. When individual information system usage or need-to-know changes.
>
> …
>
> j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].

USADF's IT Access Controls Policy, dated March 20, 2018, describes USADF's access control policies and procedures and includes requirements to notify account managers:

- When accounts are no longer required;
- When users are terminated or transferred; and

- When individual information system usage or need-to-know changes.

However, the policy did not include comparable access controls and account management policies and procedures for applications run by the following shared service providers:

- Department of Treasury / Bureau of Fiscal Services,
- Interior Business Center (IBC)/ Department of Interior (DOI), and
- Internet based shared service providers.

Further, a procedure was not in place at neither USADF nor IBC/DOI to cross-check and confirm that employees or contractors who were not working with or at USADF needed to have their access immediately terminated. For example, a judgmentally selected sample of 16 USADF personnel listed as Personal Identification Verification (PIV) credential holders from a population of 72 in the service provider's system revealed an instance where an account credential was created for an individual that was not a USADF employee.

USADF did not consider it a requirement to document the access controls and account management procedures for its shared service providers, since the shared service providers approved the user's access to the application. Without effective access and account management controls, USADF's information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. Further, user accounts that are not timely disabled when employees separate may be misused or susceptible to a 'brute force' attack to gain access to the Foundation's data and sensitive information.

A recommendation addressing this finding was issued in the FY 2017 audit. Because USADF management had not taken final corrective action, we are not making an additional recommendation at this time.[4]

USADF Needs to Update Its Access Control Policies and Procedures to include the Use of Personal Identity Verification Credentials

On August 27, 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." The directive mandates the implementation of a Governmentwide standard for secure and reliable forms of identification for Federal employees and contractors requiring physical access to federally controlled facilities and logical access to federally controlled information systems.

U.S. Department of Homeland Security memorandum "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011, states:

> Effective the beginning of FY 2012, existing physical and logical access control systems must be upgraded to use PIV [Personal Identity Verification] credentials, in accordance

[4] Recommendation 4, *The United States African Development Foundation Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed* (Audit Report A-ADF-18-001-C October 2, 2017).

with NIST [National Institute of Standards and Technology] guidelines, prior to the agency using development and technology refresh funds to complete other activities.

NIST SP 800-53, Revision 4, security control IA-2, Identification and Authentication, control enhancement (12) states:

> The information system accepts and electronically verifies Personal Identity Verification credentials.
>
> Supplemental guidance: This control enhancement applies to organizations implementing logical access control systems and physical access control systems. Personal Identity Verification credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

During August 2018, USADF implemented the use of PIV cards for gaining logical access to its internal information systems. In addition, USADF implemented Identity Access Management single-sign-on using its PIV cards for logical access to systems operated by its shared service providers.

Although USADF had implemented the use of PIV cards for logical access, it had not yet updated its access control policies and procedures to include their use. Consequently, USADF faces an increased risk that access controls over the use of PIV cards will not be consistently implemented or effective.

> **Recommendation 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.

USADF Needs to Update Its Continuous Monitoring Policy and Procedures to Include Specific Daily Continuous Monitoring Responsibilities

NIST SP 800-53, Revision 4, security control CA-7, Continuous Monitoring, states the following:

> The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
>
> a. Establishment of [Assignment: organization-defined metrics] to be monitored;
> b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
> c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
> d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

NIST SP 800-*137 Information Security Continuous Monitoring (ISCM) for Federal information Systems and Organizations*, Section 3.4.2 Report on Security Control Assessments, states:

> Organizations define security status reporting requirements in the ISCM strategy. This includes the specific staff/roles to receive ISCM reports, the content and format of the reports, the frequency of reports, and any tools to be used.

USADF in recent years has undergone major changes in its IT assets and data hosting and processing activities. As part of the management of its systems development life cycle, the Foundation has adopted and implemented policies and operating procedures that strengthen its actions and likely outcomes in the areas of security and privacy controls implementation. For example, USADF's leadership holds monthly Continuous Monitoring meetings to provide visibility into USADF's assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. In doing so, the Foundation is effectively implementing its Continuous Monitoring program.

Further, USADF's Continuous Monitoring Plan defines the roles and responsibilities of IT management to conduct monitoring on a weekly basis. For example, the continuous monitoring plan states:

1. USADF utilizes an automated tool to monitor event logs. Events from the tool will be reviewed on a weekly basis and a network access report will be prepared identifying users accessing the network and failed logon attempts.
2. The USADF utilizes an automated tool to monitor network traffic. The USADF IT department will review the system output on a weekly basis and report all anomalies to the Director of IT.
3. The USADF IT department will utilize centralized tools to monitor the status of the anti-virus on all windows based workstations on a weekly basis to ensure that the latest virus definitions are installed, working as intended and review alerts for sign of infection.

However, based on our review of USADF's continuous monitoring policies, interviews with the USADF IT team, and our observations of their operations, the daily responsibilities of the following roles were not clearly defined, described, and documented: Chief Information Security Officer, IT Systems Administrator, and IT Security Analyst. For example, their responsibilities for gathering, documenting, assessing, and remediating USADF's IT vulnerabilities, threats, and risks in a timely manner have not been documented.

USADF did not consider it a requirement to document the USADF IT department's daily continuous monitoring responsibilities, since the USADF IT department held regular meetings to discuss current threats. Not responding to identifiable threats and vulnerabilities in a timely manner at the organizational, IT asset, and user levels results in an increased probability of

negative impacts on USADF's operations due to undetected and uncorrected breaches to the confidentiality, integrity, and availability of its information systems.

Recommendation 3: We recommend 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.

Evaluation of Management Comments

In response to the draft report, the United State African Development Foundation accepted all three recommendations and provided target dates for completion. Based on our evaluation of management comments, we acknowledge management decisions on all three recommendations.

Scope and Methodology

Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *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 selected security controls for certain information systems [5] in support of the Federal Information Security Modernization Act of 2014.

Our overall objective was to evaluate USADF's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of USADF's IT security program in accordance with U.S. Department of Homeland Security's (DHS) FISMA Inspector General reporting requirements:

- Risk Management;
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of USADF's IT security governance structure and the Foundation's system security assessment and authorization (SA&A) methodology. We also followed up on outstanding recommendations from prior FISMA audits (see Appendix II), and performed audit procedures on USADF's internal system and on 6 of 8 external systems. The audit also included a vulnerability assessment of USADF-managed internal system and an evaluation of USADF's process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed USADF's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also audited an internal system and USADF's SA&A process. We considered the internal control structure for USADF's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over USADF's internal system and 6 contractor-owned and managed systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate

[5] See Appendix IV for a list of controls selected.

internal controls were designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to USADF's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the FYs 2017, 2016 and 2015 FISMA audit reports; and
- Completed a network vulnerability assessment of USADF's internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for USADF's systems taken as a whole.

The criteria used in conducting this audit included:

- Public Law 113-283, Federal Information Security Modernization Act of 2014;
- FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- NIST SP 800-12, Revision 1, *An Introduction to Computer Security*: The NIST Handbook;
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors;* and

- Other criteria as appropriate.

The audit was conducted at USADF's headquarters in Washington, D.C., from April 16, 2018 through September 7, 2018.

Status of Prior Year Findings

No.	FY 2017[6], 2016[7] and 2015[8] USADF FISMA Audit Recommendations and Disposition	Status	Auditor's Position on Status
1	***FY 2017 FISMA audit recommendation No. 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 associated with the operation and use of the Foundation's information systems in accordance with National Institute of Standards and Technology standards.*	Open (Partially Completed)	Agree USADF has started, but not fully documented an organization-wide risk management strategy.
2	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.*	Closed.	Agree
3	c. *Perform information system security assessments on an annual basis in accordance with the Foundation's policy.*	Closed.	Agree

[6] *The United States African Development Foundation Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed (Audit Report A-ADF-18-001-C October 2, 2017).*
[7] *The United States African Development Foundation's Information Security Program Needs Improvements to Comply with FISMA* (Audit Report No. A-ADF-17-002-C, November 7, 2016).
[8] *Audit of the U.S. African Development Foundation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-ADF-16-002-P, November 13, 2015).

4	d. *Review and update the system risk assessments to take into account 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.*	Open (Partially Completed)	Agree USADF has not fully updated the system risk assessments to ensure the authorizing official has appropriate knowledge of the state of the information systems' security.
5	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
6	***FY 2017 FISMA audit recommendation No. 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 in accordance with the USADF's policy. This includes confirming patches are applied in a timely manner and tested prior to implementation in accordance with USADF policy.*	Open (Partially Completed)	Agree USADF has developed a process to track and remediate vulnerabilities, but the process does not include confirming that patches are applied in a timely manner and tested prior to implementation in accordance with USADF policy.
7	***FY 2017 FISMA audit recommendation No. 3:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to migrate unsupported applications from their existing platform to vendor-supported platforms. That process must document the risks, required approvals, and adequate mitigating controls for unsupported software until it can be migrated to vendor-supported platforms.*	Closed.	Agree
8	***FY 2017 FISMA audit recommendation No. 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.*	Open (Partially Completed)	Agree USADF has started, but not fully documented a written process to enforce the immediate disabling of employee user accounts upon separation from the organization and perform account recertification.

9	***FY 2016 FISMA audit recommendation No. 2.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to review and update 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 process should include determining whether the security requirements and controls for the system are adequately documented and reflect the current information system environment.*	Closed.	Agree
10	***FY 2016 FISMA audit recommendation No. 3.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to perform security assessments in accordance with National Institute of Standards and Technology standards. This process should include documenting assessment procedures to be used to determine security control effectiveness and testing the operating effectiveness of security controls.*	Closed.	Agree
11	***FY 2016 FISMA audit recommendation No. 4.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process for assessing risk in internal and cloud service provider's systems—taking into account all known vulnerabilities and threat sources, security controls planned or in place, and residual risk— to make the authorizing official for each system aware of its security state.*	Closed.	Agree
12	***FY 2016 FISMA audit recommendation No. 6.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to develop, communicate, and implement an organization-wide risk management strategy associated with the operation and use of the Foundation's information systems in accordance with National Institute of Standards and Technology standards.*	Closed.	Agree

13	***FY 2016 FISMA audit recommendation No. 10.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to track and remediate vulnerabilities timely in accordance with the Foundation's policy. This process should include ascertaining that patches are tested before being put into production and applied promptly in accordance with policy.*	Closed.	Agree .
14	***FY 2016 FISMA audit recommendation No. 11.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to migrate unsupported applications to platforms supported by vendors. For unsupported applications that cannot be migrated immediately, this process must include documenting the risk of leaving them on their current platforms, acceptance of that risk and compensating controls that will be used until migration is possible.*	Closed.	Agree
15	***FY 2016 FISMA audit recommendation No. 23.*** *We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to reevaluate the security categorization of the general support, travel, and human resources systems in accordance with the Office of Management and Budget and National Institute of Standards and Technology guidance given that the systems contain personally identifiable information.*	Closed.	Agree
16	***FY 2015 FISMA audit recommendation No. 3.*** *We recommend that the United States African Development Foundation's Chief Financial Officer develop and implement a documented process to review and update the USADF General Support System's System Security Plan on an annual basis. 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.*	Closed.	Agree

17	***FY 2015 FISMA audit recommendation No. 10.*** *We recommend that the United States African Development Foundation's Chief Financial Officer update the Contingency Plan for the General Support System and Program Support System to reflect the transition to cloud-based service providers.*	Closed.	Agree

Management Comments

October 15, 2018

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 2018 (Report No. A-ADF-19-00X-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 fully develop and document a risk management strategy for information technology operations that requires the Foundation to identify: (1) risk assumption; (ii) risk constraints (iii) risk tolerance; and (iv) priorities and trade-offs.

We accept the recommendation 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 assumptions (ii) risk constraints (iii) risk tolerance; and (iv) priorities and trade-offs. Final action on this finding and recommendation will be completed by December 31, 2018.

Recommendation No. 2: We recommend that the United States African Development Foundation's 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.

> We accept the recommendation 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. Final action on this finding and recommendation will be completed by January 31, 2019.

Recommendation No. 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.

> We accept the recommendation 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. Final action on this finding and recommendation will be completed by November 30, 2018.

/s/

C.D. Glin
President

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

Number of Controls Reviewed for Each System

Control No.	Control Name	Number of Systems Tested
AC-1	Access Control Policy & Procedures	1
AC-2	Account Management	6
AC-8	System Use Notification	1
AC-17	Remote Access	2
AT-1	Security Awareness & Training Policy and Procedures	1
AT-2	Security Awareness	2
AT-3	Role-Based Security Training	2
AT-4	Security Training Records	1
AU-9	Protection of Audit Information	1
CA-1	Security Assessment and Authorization Policy & Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	1
CA-6	Security Authorization	1
CA-7	Continuous Monitoring	1
CM-2	Baseline Configuration	1
CM-8	Information System Component Inventory	1
CP-1	Contingency Planning Policy & Procedures	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing and Exercises	1
IA-1	Identification & Authentication Policy and Procedures	1
IA-4	Identifier Management	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
PE-1	Physical and Environmental Protection Policy and Procedures	1
PE-2	Physical Access Authorizations	1
PL-2	System Security Plan	2
PM-5	Information System Inventory	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 & Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1

Control No.	Control Name	Number of Systems Tested
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	1
RA-3	Risk Assessment	6
SA-4	Acquisitions Process	1
SA-9	External Information System Services	6
SI-2	Flaw remediation	1
	TOTAL CONTROLS	**59**

Acronyms

DHS	U.S. Department of Homeland Security
DOI	Department of Interior
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IBC	Interior Business Center
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SA&A	Security Assessment and Authorization
SP	Special Publication
USADF	U.S. African Development Foundation