OFFICE OF INSPECTOR GENERAL
U.S. African Development Foundation

USADF Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed

AUDIT REPORT A-ADF-18-001-C
OCTOBER 2, 2017

1300 Pennsylvania Avenue NW • Washington, DC 20523
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

U.S. African Development Foundation Hotline
Email: adfhotline@usaid.gov
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG, Attn: USADF Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: October 2, 2017

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

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

SUBJECT: USADF Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed (A-ADF-18-001-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 2017. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. The contract required Clifton to perform the audit in accordance with generally accepted government auditing standards.

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

The audit objective was to determine whether USADF implemented certain security controls for selected information systems consistent with FISMA. To answer the audit objective, Clifton 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." Clifton auditors reviewed all seven systems in USADF's inventory as of March 13, 2017. Fieldwork took place at USADF's headquarters in Washington, DC, from March 8 to July 25, 2017.

Clifton concluded that USADF implemented 71 of 91 selected security controls designed to preserve the confidentiality, integrity, and availability of its information and information systems. For example, USADF did the following:

- Implemented an effective process to monitor, review, and analyze audit logs.
- Implemented an effective general and role-based security awareness training program.
- Maintained an effective program for incident handling and response.
- Documented and implemented an enterprise architecture.
- Documented approved deviations from the U.S. Government Configuration Baseline settings and implemented a process to check for compliance.
- Implemented multifactor authentication for network access to privileged accounts.
- Implemented a process to maintain the inventory of information system components.

However, USADF did not completely implement the remaining 20 security controls.

Clifton made and OIG agrees with the following recommendations to USADF's management to address the weaknesses identified; we will track the recommendations until USADF fully implements them. We recommend USADF's chief information security officer:

Recommendation 1. Strengthen the organization-wide information security program in accordance with National Institute of Standards and Technology standards by establishing and implementing documented processes to:

- Establish, communicate, and implement an organization-wide risk management strategy for operation and use of the Foundation's information systems in accordance with National Institute of Standards and Technology standards.
- 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.
- Perform information system security assessments on an annual basis in accordance with USADF's policy.
- Review and update the system risk assessments to account for all known vulnerabilities, threat sources, and security controls planned or in place, and determine the residual risk to ensure the authorizing official has appropriate knowledge of the state of the information systems' security.
- Identify all known security weaknesses, associated corrective plans, and estimated completion dates in the plan of action and milestones, and demonstrate recommendations are effectively remediated prior to closing them.

Recommendation 2. Develop and implement a documented process to track and remediate vulnerabilities in accordance with USADF's policy. This includes confirming patches are applied in a timely manner and tested prior to implementation in accordance with USADF policy.

Recommendation 3. 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 that will be used for unsupported software until it can be migrated to vendor-supported platforms.

Recommendation 4. 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.

In finalizing the report, Clifton evaluated USADF's responses to the recommendations. Both Clifton and OIG acknowledge USADF's management decisions on all four recommendations.

We appreciate the assistance extended to our staff and Clifton employees during the engagement.

CliftonLarsonAllen

United States African Development Foundation Needs to Strengthen its Organization-Wide Information Security Program to Comply with the Federal Information Security Modernization Act of 2014

Fiscal Year 2017

Final Report

CliftonLarsonAllen

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

September 22, 2017

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:

Enclosed is the final version of our report on the United States African Development Foundation's (USADF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The United States African Development Foundation Needs to Strengthen its Organization-Wide Information Security Program to Comply with the Federal Information Security Modernization Act of 2014*. The USAID Office of Inspector General contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP 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 certain security controls for selected 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 the entire population of seven USADF information systems as of March 13, 2017. This included one internal and six external systems. The audit also included a vulnerability assessment of USADF's general support system and an evaluation of USADF's process for identifying and correcting/mitigating technical vulnerabilities. The audit fieldwork was performed at USADF's headquarters in Washington, D.C., from March 8, 2017, through July 25, 2017.

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 implemented 71 of 91 security controls reviewed for selected information systems in support of FISMA. Although USADF generally had policies for its information security program, its implementation of those policies for 20 of 91 security 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. Consequently, the audit identified areas in USADF's information security program that needed to be improved. We are making 4 recommendations to assist USADF in strengthening its information security program.

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.

Very truly yours,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

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, including those provided or managed by another agency, contractor, or other source. Because the United States African Development Foundation (USADF) is a federal agency, it is required to comply with federal information security requirements.

The act 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 are mandatory for federal agencies.

The U.S. Agency for International Development's Office of Inspector General engaged us, CliftonLarsonAllen LLP, 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 certain security controls for selected information systems[2] 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 the entire population of seven USADF information systems[3] as of March 13, 2017. This included one internal 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 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] See Appendix III for a list of controls reviewed.

[3] 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

The audit concluded that USADF implemented 71 of 91 security controls reviewed for selected information systems in support of FISMA. For example, USADF:

- Implemented effective audit log monitoring, review and analysis.
- Implemented an effective general and role based security awareness training program.
- Maintained an effective program for incident handling and response.
- Documented and implemented an enterprise architecture.
- Documented approved deviations from the United States Government Configuration Baseline settings and implemented a process to check for compliance.
- Implemented multifactor authentication for network access to privileged accounts.
- Implemented a process to maintain the inventory of information system components.

In addition, USADF implemented four fiscal year (FY) 2015 and 18 FY 2016 audit recommendations, two of which were implemented during audit fieldwork. Therefore, since USADF completed the corrective action we did not fully develop findings related to those recommendations in this report. See Appendix IV for a listing of the two recommendations that were implemented during fieldwork.

Although USADF had policies for its information security program, its implementation of those policies was not always 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. The audit found that USADF had not effectively implemented 20 of 91 security controls and identified the following actions that USADF needs to take to correct the weaknesses in its information security program:

- Develop and fully implement an entity-wide program for managing risk associated with the operation and use of the foundation's information systems.
- Perform security assessments and authorizations of systems in accordance with National Institute of Standards and Technology (NIST) standards and OMB guidance, including conducting security control assessments and updating system security plans (SSPs) and risk assessments in accordance with NIST standards.
- Develop and fully implement a documented process to ensure that plan of action and milestones (POA&Ms) for two systems include all known security control weaknesses and are adequately documented.
- Develop and fully implement a documented process to ensure that weaknesses identified in vulnerability scans are remediated timely and patches are consistently tested in accordance with USADF policy.

- Develop and fully implement a documented process to ensure the foundation's account management policies are adhered to.
- Develop and fully implement a documented process to ensure multifactor authentication is implemented and enforced for local and network access.

We made four recommendations to assist USADF in strengthening its information security program. In response to the draft report, USADF outlined and described its plans to address all four audit recommendations. Based on our evaluation of their comments, we acknowledge management decisions on all recommendations. USADF's comments are included in their entirety in Appendix II.

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

AUDIT FINDINGS

1. USADF Needs to Strengthen the 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 Special Publication (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.

USADF had not fully implemented an organization-wide information security program. Specifically, weaknesses were noted in the following program management controls tested:

- Risk Management Strategy
- Security Authorization Process
  - System Security Plans
  - Security Control Assessments
  - Risk Assessments
- Plan of Action and Milestones Process

Risk Management Strategy

NIST SP 800-53, Revision 4, security control PM-9, 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.

In fiscal year (FY) 2016, USADF did not develop, document and communicate an entity-wide program for managing risk associated with the operation and use of the foundation's information systems in accordance with NIST and their own policy. In FY 2017, although USADF officially closed the recommendation from the FY 2016 audit,[4] they had not made progress on developing an entity-wide risk management strategy. According to the Chief Information Security Officer (CISO), emphasis was placed on assessing risk at the information system level rather than an entity-wide program.

Without developing, documenting and communicating an organization-wide risk strategy, information technology strategic goals, objectives and 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 the confidentiality, integrity and availability of the foundation's information.

Security Authorization Process

NIST SP 800-53, Revision 4, security control PM-10, states the following regarding the security authorization process:

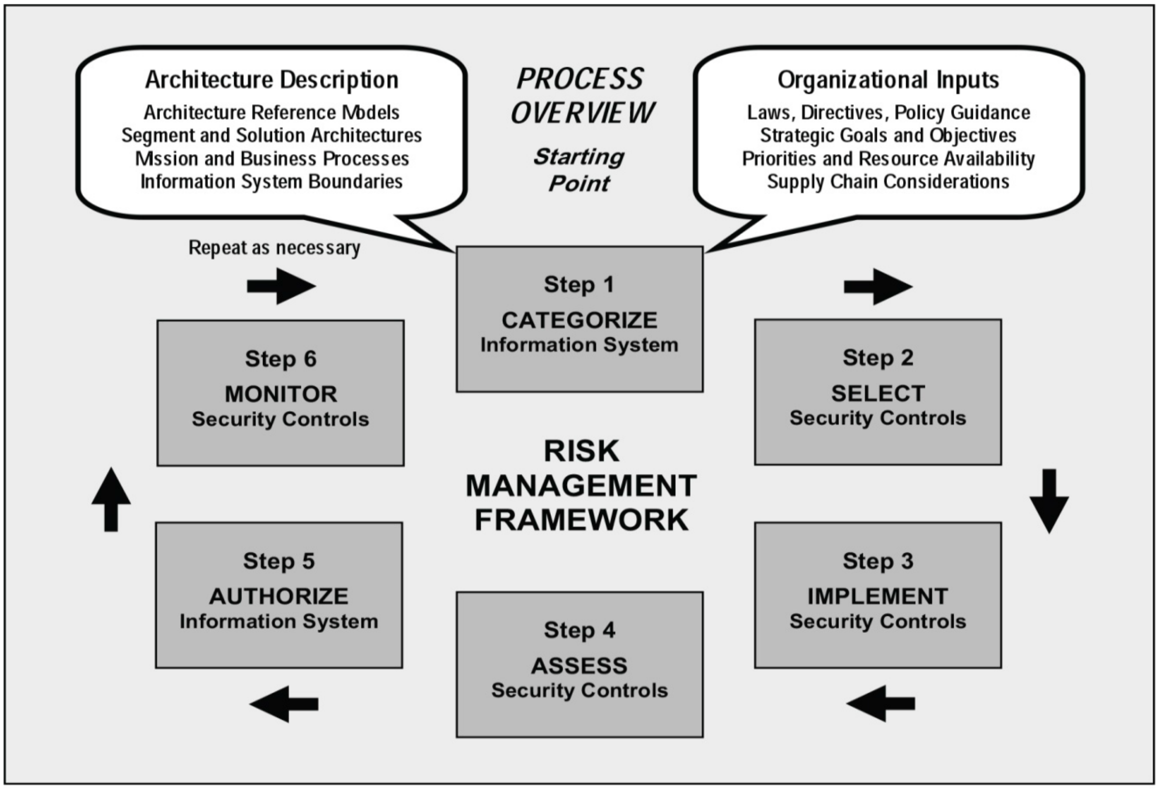
> The organization:
>
> a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes.

NIST's Risk Management Framework (RMF) provides the structure for the security authorization of federal information systems. The process includes selecting and implementing security controls for the information system and describing how the controls are implemented in the SSP; assessing whether the controls are operating as intended; analyzing and assessing risk to the information system based on weaknesses and vulnerabilities identified; and authorizing the information system based on the determination of risk.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the RMF to Federal information systems. This framework is detailed in the following figure.

[4] Recommendation 6, *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).

NIST Risk Management Framework


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mssion and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Source: NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

NIST SP 800-37, Revision 1 states:

> The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions.

During FY 2017, USADF issued an Authorization to Operate (ATO) for one system, but we identified issues with the SSP and risk assessment as discussed on the following pages. In addition, the security assessment and authorization documentation for another system had not been updated on an annual basis as required by USADF policy. Although recommendations addressing these issues were made in the FYs 2015[5] and 2016 FISMA audit reports,[6] the actions taken to address them were insufficient.

[5] Recommendations 1, 2, 3, 4 and 5, *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).

[6] Recommendations 2, 3, 4, and 5, *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).

System Security Plans

NIST SP 800-53, Revision 4, security control PL-2, states the following regarding SSPs:

> The organization:
>
> a. Develops a security plan for the information system that:
>
> …
>
> 2. Explicitly defines the authorization boundary for the system;
>
> …
>
> 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

Recommendations to review and update the SSP for one system were made in the FYs 2015[7] and 2016[8] audits, and USADF reported that they took final corrective action and closed both. However during this audit, we noted the SSP for that same system and another system were not documented in accordance with NIST requirements. For example:

- The SSP for one system did not specify the accreditation boundary. Specifying the information system boundary is key in the risk management and security authorization process to ensure risk was properly assessed and evaluated. In addition, the control implementation descriptions were not completely documented for 31 from the total population of 115 controls included in the SSP.
- For the other system, although the SSP was updated since last year, we continued to note discrepancies. For example, six controls were documented as implemented; however, the control implementation descriptions stated that controls were not implemented or not applicable. In addition, the control implementation descriptions were not completely documented for 14 of the 132 security controls.
- The SSPs for the two systems did not describe the implementation of privacy controls specified in NIST SP 800-53, Revision 4, Appendix J. A recommendation to develop and fully implement a documented process to review and update SSPs to reflect NIST Special Publication 800-53, Revision 4, was made in the FY 2016 audit.[9] USADF closed the recommendation, though full corrective action was not taken.

[7] Recommendation 3, *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).

[8] Recommendation 2, *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).

[9] Recommendations 10 and 11, *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).

This occurred because the CISO did not monitor the work performed by the contractor to ensure the security requirements and controls were adequately documented and reflected the current information system environment. In addition, the CISO stated the privacy controls will be addressed in a separate document. Finally, the CISO specified that since one of the systems is now Federal Risk and Authorization Management Program (FedRamp) approved and the vendor is responsible for the majority of security controls, USADF will be consolidating common system security controls such as account management into one SSP.

Without complete and up-to-date SSPs, USADF systems could be susceptible to unknown security risks resulting from changes to the environment.

<u>Security Control Assessments</u>
NIST SP 800-53, Revision 4, security control CA-2, states the following regarding security control assessments:

> The organization:
>
> …
>
> b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

In addition, the *USADF Information Technology Security Implementation Plan* states:

> The USADF will establish the selection criteria and subsequently, select a subset of the security controls (approximately one third of the total security controls) that will be assessed each year for all USADF systems.

USADF did not conduct an annual assessment of the security controls for one of the two systems tested as required by USADF policy. The last assessment was conducted on August 31, 2015. The CISO indicated that since that system is now FedRamp approved and a Service Organization Control (SOC) report details the results of control assessments, going forward USADF will rely on the results of the SOC report and conduct a limited assessment of controls, such as account management that USADF is responsible for.

Without assessing the operating effectiveness of security controls on a continuous basis, USADF was not able to confirm controls were operating effectively, and the foundation may be at risk of information loss, fraud or abuse.

Risk Assessments

NIST SP 800-53, Revision 4, security control RA-3, states the following regarding system risk assessments:

> The organization:
>
> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

In addition, the *USADF Information Technology Security Implementation Plan*, states:

> Risk assessments shall take into account vulnerabilities, threat sources, and security controls planned or in place, to determine the resulting level of residual risk posed to USADF operations, assets, or individuals based on the operation of the information system. This includes risks posed from external parties, including:
>
> - Service providers;
> - Contractors operating and maintaining information systems on behalf of USADF;
> - Individuals accessing USADF information systems; and
> - Outsourced entities (e.g., other government entities).

Although, USADF documented an acceptance of the risks for using a major external application, the SOC report reviewed was for the period October 1, 2014 to June 30, 2015. Therefore, the risk assessment did not take into account current system risks. The CISO indicated a current SOC report for that major application was not available for review.

In addition, seven controls that were documented as partially implemented or planned in the SSP for one system were not addressed in the system risk assessment dated May 24, 2017. Further, none of the controls listed as planned in the SSP for one system were documented and analyzed in the risk assessment. This occurred because the CISO did not monitor the work performed by the contractor to ensure all partially implemented or planned controls in the SSPs were included in the system risk assessments.

The lack of adequately documented risk assessments increases the risk that the authorizing official will not have the appropriate knowledge to ensure mitigation of known risks and make an informed risk-based decision on whether to authorize the system to operate.

Plan of Action and Milestones Process

NIST SP 800-53, Revision 4, security control PM-4, states the following regarding the POA&M management process:

> The organization:
>
> a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
>   1. Are developed and maintained;
>   2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation.

In addition, the *USADF Information Technology Security Implementation Plan*, states:

- USADF shall develop and update a Plan of Actions and Milestones to track and mitigate all system weaknesses and/or deficiencies.

USADF's POA&M management process had weaknesses for two systems. Specifically:

- For one system, 39 of the 45 planned controls listed in the SSP were not included in the POA&Ms.
- For another system, the entire population of POA&Ms resulting from the most recent security control assessment did not include estimated completion dates and corrective action plans.

The CISO did not adequately review and monitor the POA&Ms to ensure the authorizing official had current and on-going information regarding the security state of the foundation's information systems. This involves ensuring POA&Ms include all known security weaknesses, estimated completion dates and associated corrective action plans.

Furthermore, USADF closed eight prior year audit recommendations without validating adequate remediation was performed. See Appendix V for a listing of those recommendations. The CISO did not sufficiently review supporting documentation to substantiate the recommendations were effectively remediated prior to closing them.

Without documenting and tracking all known system security control weaknesses including associated scheduled completion dates and corrective actions in the POA&Ms, and without substantiating recommendations were effectively remediated prior to closing them, USADF remained susceptible to system security risks.

Strengthening the foundation's organization-wide information security program is key to reducing the risk associated with the use of information systems that support USADF's operations. Because USADF officially closed the recommendations related to the organization wide information security program from the FY 2016 audit,[10] we are issuing a new recommendation as follows:

> ***Recommendation 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.*
> *b. Review and update the system security plans to reflect National Institute of Standards and Technology Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations*. At a minimum, this should include a determination whether the security requirements and controls for the system are adequately documented and reflect the current information system environment.*
> *c. Perform information system security assessments on an annual basis in accordance with the foundation's policy.*
> *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.*
> *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.*

2. Vulnerability Management Controls Need Strengthening

NIST SP 800-53, Revision 4, security control RA-5 states the following regarding vulnerability scanning:

> The organization:
>
> …
>
> b. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk.

[10] Recommendations 2, 3, 4, 5, and 6, *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).

Security control SI-2 states the following regarding flaw remediation:

> The organization:
>
> a. Identifies, reports, and corrects information system flaws;
> b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

In addition, the USADF *Information Technology Security Implementation Plan*, RA-5 states:

> USADF shall analyze and remediate all findings within a three month period. All residual vulnerabilities that cannot be remediated within a three month period shall be documented in the system POA&M.

Also, *USADF Patch Management Procedures* require testing of patches prior to implementation into production.

Weaknesses were noted with USADF's vulnerability management process. Specifically, USADF did not remediate vulnerabilities timely in accordance with USADF policy and did not address unsupported software. Specifically:

- Independent authenticated scans of 30 of the 100 hosts using the software tool Nessus, noted 103 unique critical and high risk vulnerabilities related to patch management and insecure configurations. Although, USADF tracked the vulnerabilities in POA&Ms and updated the status on a quarterly basis, they were not remediated at the time of testing.
- Independent scans also identified 35 unique instances of critical vulnerabilities, due to software which was no longer supported by a vendor. The CISO was aware of and accepted the risk for using three of the four software applications.
- USADF did not consistently follow their patch management procedures. Although, the CISO provided evidence of testing for the January 2017 patches for one software application, evidence was not provided for the remaining months during the audit period to validate a repeatable process was in place. Without testing patches, there is an increased risk that the normal operation of the software may be affected causing disruption to the production system.

The CISO did not provide satisfactory supervision to ensure that vulnerabilities were remediated timely in accordance with USADF policy, including testing of patches. Furthermore, the CISO did not implement a process to migrate unsupported applications from their existing platform to platforms that are vendor-supported. Overall, vulnerability assessment and timely flaw remediation was not given the proper priority in the configuration management process.

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

The 2016 audit report made recommendations to address these weakness.[11] Because USADF officially closed them, we are issuing new recommendations to correct the weaknesses related to USADF's vulnerability management.

> ***Recommendation 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.*
>
> ***Recommendation 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 platforms that are vendor-supported. That process must include documenting the risk and granting approval, including adequate compensating controls, if an exception must be made until the unsupported software is migrated to vendor-supported platforms.*

3. Account Management Controls Need Strengthening

NIST SP 800-53, Revision 4, security control AC-2, 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].
>
> …
>
> 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].

We noted the following account management issues:

- Accounts for two out of the entire population of six separated employee's were not disabled.
- We were not able to validate that a user account recertification was performed for three of the seven systems tested due to lack of evidence provided.

The *USADF Information Technology Security Implementation Plan* did not address the timeline for disabling user accounts when employees separate, or the required frequency for recertifying accounts. In addition, the CISO specified that although a

[11] Ibid. footnote 09.

mechanism was in place to notify IT when employees are separating, management directed IT to keep these two accounts enabled for a period of time in case the accounts needed to be accessed. In addition, the CISO indicated a response was not required from USADF managers if their review of system accounts resulted in no necessary access changes. Requiring a response from the USADF managers would have validated a review was performed.

Without effective access controls, USADF information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. User accounts that are not 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.

> ***Recommendation 4:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to implement and enforce the disabling of user accounts immediately when employees separate and performing account recertification in accordance with foundation policy, including the required frequency for recertifying accounts and the process for providing responses.*

4. Multifactor Authentication for Non-Privileged Accounts Needs to be Fully Implemented

Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004) requires the use of Personal Identification Verification for gaining logical access to federally controlled information systems. NIST 800-53, Revision 4, defines system access to organizational information systems as either local access or network access.

NIST SP 800-53, Revision 4, security control IA-2, 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.

Personal Identity Verification (PIV) credentials were not implemented for local and network access for non-privileged accounts. The *USADF Information Technology Security Implementation Plan* did not require the use of PIV credentials. In addition, the CISO indicated that although the foundation had obtained the PIV cards, management concluded it was cost prohibitive at this time to implement the technology.

By not implementing multifactor authentication for local and network access, USADF increases the risk that unauthorized individuals could gain access to its information system and data.

The 2016 audit report made a recommendation to implement and enforce the use of PIV credentials for access to the foundation’s facilities, computers, and network.[12] USADF subsequently implemented PIV access for the facility, but did not close this recommendation due to the lack of implementation of multifactor authentication for local and network access. Therefore, we are not making a new recommendation at this time.

[12] Recommendation 20, *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).

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the USADF described planned actions to address all four recommendations. USADF's comments are included in their entirety in Appendix II.

Based on our evaluation of their comments, we acknowledge management decisions on all four 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 the USADF implemented certain security controls for selected information systems[13] in support of FISMA.

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

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

For this audit, we reviewed the entire population of seven USADF information systems as of March 13, 2017. See Appendix III for a listing of selected controls. The audit also included a vulnerability assessment and an evaluation of USADF's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit

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

included a follow up on prior year audit recommendations[14] to determine if USADF made progress in implementing the recommended improvements concerning its information security program.

The audit was conducted at USADF's headquarters in Washington, D.C., from March 8, 2017, through July 25, 2017.

Methodology

Following the framework for minimum security controls in NIST SP 800-53, Revision 4, certain controls (listed in Appendix III) were selected from NIST security control families.[15] We reviewed selected controls[16] for seven systems.

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, SSPs, security control assessments, risk assessments, plan of action and milestones, incident response plan, configuration management plan and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix III).
- Completed a vulnerability assessment of one USADF system and evaluated USADF's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of USADF vulnerability scanning configurations and results and comparing them with independent network vulnerability scan results.
- Reviewed the status of recommendations in the FY 2015 and FY 2016 FISMA audit reports, including supporting documentation to ascertain whether the actions taken addressed the weakness.[17]

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

[14] 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) and *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).

[15] Security controls are organized into families according to their security function—for example, access controls.

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

[17] Ibid. footnote 17.

MANAGEMENT COMMENTS

September 12, 2017

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 2017 (Report No. A-ADF-17-00X-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 strengthen the organization-wide information security program in accordance with National Institute of Standards and Technology standards by establishing and implementing documented processes to:

- Establish, communicate and implement an organization wide risk management strategy for operation and use of the foundation's information systems in accordance with National Institute of Standards and Technology standards.
- 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.
- Perform information system security assessments on an annual basis in accordance with USADF's policy.
- Review and update the system risk assessments to account for all known vulnerabilities, threat sources, and security controls planned or in place, and

determine the residual risk to ensure the authorizing official has appropriate knowledge of the state of the information systems' security.

- Identify all known security weaknesses, estimated completion dates and associated corrective plans in the plan of action and milestones and demonstrate recommendations are effectively remediated prior to closing them.

> We accept the recommendation that the United 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 establishing and implementing documented processes to:
>
> - Establish, communicate and implement an organization-wide risk management strategy for operation and use of the foundation's information systems in accordance with National Institute of Standards and Technology standards.
> - Review and update the system security plans to reflect National Institute of Standards and Technology Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." At a minimum, this will include a determination with the security requirements and controls for the system are adequately documented and reflect the current information system environment.
> - Perform information system security assessment on an annual basis in accordance with USADF's policy.
> - Review and update the system risk assessments to account for all known vulnerabilities, threat sources, and security controls planned or in place, and determine the residual risk to ensure the authorizing official has appropriate knowledge of the state of the information systems' security.
> - Identify all known security weaknesses, estimated completion dates and associated corrective plans in the plan of action and milestones and demonstrate recommendations are effectively remediated prior to closing them.
>
> Final action on this finding and recommendation will be completed by April 30, 2018.

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.

> We accept the recommendation that the United 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. Final action on this finding and recommendation will be completed by January 15, 2018.

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.

> We accept the recommendation 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 will document the risks, required approvals, and adequate mitigating controls for unsupported software until it can be migrated to vendor - supported platforms. Final action on this finding and recommendation will be completed by March 15, 2018.

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.

> We accept the recommendation 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. Final action on this finding and recommendation will be completed by November 1, 2017.

/s/
C.D. Glin
President

cc:

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

SUMMARY OF CONTROLS REVIEWED

The following table provides a summary of the controls selected for review for the FY 2017 audit. We did not review each control for each system. Additional controls were reviewed as a result of follow up testing for prior year recommendations.

Control No.	Control Name	# of Systems Reviewed
AC-1	Access Control Policy and Procedures	1
AC-2	Account Management	6
AC-3	Access Enforcement	1
AC-5	Separation of Duties	1
AC-7	Unsuccessful Login Attempts	1
AC-17	Remote Access	2
AC-19	Access Control for Mobile Devices	1
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness	2
AT-3	Security Training	2
AU-2	Audit Events	1
AU-6	Audit Review, Analysis, and Reporting	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	1
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policy and Procedures	1
CM-2	Baseline Configuration	1
CM-4	Security Impact Analysis	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	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 and Exercises	1
CP-7	Alternate Processing Site	1
CP-9	Information System Backup	1
CP-10	Information System Recovery and Reconstitution	1
IA-1	Identification and Authentication Policy and Procedures	1

Control No.	Control Name	# of Systems Reviewed
IA-2	Identification and Authentication (Organizational Users)	1
IA-4	Identifier Management	1
IA-5	Authenticator Management	1
IA-6	Authenticator Feedback	1
IA-7	Cryptographic Module Authentication	1
IA-8	Identification and Authentication (Non-Organizational Users)	1
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1
IR-5	Incident Monitoring	1
IR-6	Incident Reporting	1
IR-8	Incident Response Plan	1
PL-1	Security Planning Policy and Procedures	1
PL-2	System Security Plan	1
PL-4	Rules of Behavior	1
PS-1	Personnel and Security Policy and Procedures	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	1
RA-3	Risk Assessment	7
RA-5	Vulnerability Scanning	1
SA-1	System and Services Acquisition Policy and Procedures	1
SA-4	Acquisition's Process	1
SA-9	External Information System Services	7
SC-7	Boundary Protection	1
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	1
SI-2	Flaw Remediation	1
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
PM-1	Information Security Program Plan	1
PM-4	Plan of Action and Milestones Process	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-9	Risk Management Strategy	1
PM-10	Security Authorization Process	2
PM-11	Mission/Business Process Definition	1
IP-1	Consent	1
IP-4	Complaint Management	1

PRIOR RECOMMENDATIONS IMPLEMENTED DURING FIELDWORK

No.	FY 2015 Audit Recommendation[18]
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.
No.	**FY 2016 Audit Recommendation[19]**
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.

[18] *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).

[19] 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).

PRIOR RECOMMENDATIONS USADF CLOSED WITHOUT ADEQUATE REMEDIATION

No.	FY 2015 Audit Recommendation[20]
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.
No.	**FY 2016 Audit Recommendation[21]**
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.
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.
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.

[20] Ibid. footnote 22.
[21] Ibid. footnote 23.

No.	FY 2016 Audit Recommendation
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.
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.
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.
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.