OFFICE OF INSPECTOR GENERAL

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

WASHINGTON, DC

Please note that certain information contained in this transmittal memo and attached report has been redacted as "SBU" (sensitive but unclassified) by USADF officials, meaning that public disclosure of this material could compromise the integrity of government computer systems and networks. All redactions are made under Freedom of Information Act Exemption 7(E).

Office of Inspector General

November 7, 2016

The Honorable C.D. Glin
United States African Development Foundation
President and Chief Executive Officer
1400 I Street NW
Suite 1000
Washington, DC 20005

Dear Mr. Glin:

Enclosed is the final report, "The United States African Development Foundation's Information Security Program Needs Improvements To Comply With FISMA" (Report No. A-ADF-17-002-C). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit in accordance with U.S. generally accepted government auditing standards. Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it.

In carrying out our oversight responsibilities, we reviewed the report and related audit documentation to determine whether Clifton complied with U.S. generally accepted government auditing standards. Our review was different from an audit in accordance with those standards and was not intended to enable us to express, and we do not express, an opinion on the United States African Development Foundation's (USADF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). Our review did not disclose any instances in which Clifton did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USADF implemented security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested USADF's implementation of selected controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Clifton auditors reviewed the following systems: (1) General Support, (2) Program Support, (3) Payroll, (4) Human Resources, (5) PRISM, (6) Oracle Financials, and (7) Travel. Fieldwork took place at USADF's headquarters in Washington, DC, from March 3 to July 7, 2016.

Clifton concluded that USADF had not completely implemented its information security program. USADF effectively implemented 41 of the 77 selected security controls. However, USADF did not effectively implement the remaining 36 controls.

The weaknesses identified point to USADF's ineffective risk management program. In particular, security assessment and authorization were inadequate for USADF information systems, as in fiscal year 2015, resulting in a significant deficiency to information system security again this year. Office of Management and Budget Memorandum M-14-04, "Fiscal Year 2014 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or in one or more information systems that significantly restricts the agency's ability to carry out its mission or compromises the security of its information; information systems; personnel; or other resources, operations, or assets.

To help USADF strengthen its information security program, we make the following 26 recommendations.

> ***Recommendation 1.*** *We recommend that the United States African Development Foundation's president appoint in writing a senior-level chief information security officer in accordance with the Federal Information Security Modernization Act and the National Institute of Standards and Technology.*
>
> ***Recommendation 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.*
>
> ***Recommendation 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.*
>
> ***Recommendation 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.*
>
> ***Recommendation 5.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to update all known security weaknesses and associated corrective plans quarterly as required by the foundation's policy and include them in the plan of action and milestones.*

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.*

Recommendation 7. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to review and maintain an up-to-date information system inventory.*

Recommendation 8. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to develop, document, and implement an enterprise architecture in accordance with National Institute of Standards and Technology standards.*

~~(SBU)~~ ***Recommendation 9.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to perform* [redacted].

~~(SBU)~~ ***Recommendation 10.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to* [redacted] *in accordance with the foundation's policy. This process should include ascertaining that* [redacted] *in accordance with policy.*

Recommendation 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.*

~~(SBU)~~ ***Recommendation 12.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to* [redacted] *with the* [redacted] *including* [redacted].

~~(SBU)~~ ***Recommendation 13.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to* [redacted] *and* [redacted] *in the future. This process must include documenting the risk of* [redacted] *and documenting the approval of any exceptions, along with adequate compensating controls.*

Recommendation 14. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to document, approve, and disseminate approved deviations from the United States Government Configuration Baseline settings.*

Recommendation 15. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to configure and regularly monitor password settings in accordance with the foundation's policy and encrypt passwords during authentication.*

Recommendation 16. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to specify an organization-defined frequency for reviewing and updating the inventory of information system components.*

Recommendation 17. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to maintain the inventory according to policy.*

Recommendation 18. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to remove and decommission unused systems promptly.*

Recommendation 19. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to implement and enforce multifactor authentication for network access to privileged accounts.*

Recommendation 20. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to implement and enforce the use of personal identity verification credentials for access to the foundation's facilities, computers, and network.*

~~(SBU)~~ ***Recommendation 21.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to* [redacted].

Recommendation 22. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to review and analyze all required audit logs in accordance with National Institute of Standards and Technology standards and the foundation's policy.*

~~(SBU)~~ ***Recommendation 23.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to* [redacted] *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.*

Recommendation 24. *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to maintain a current interconnection security agreement and memorandum of understanding between the foundation and the U.S. Department of Interior's Interior Business Center.*

> ***Recommendation 25.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to provide annual security awareness training to overseas partners.*
>
> ***Recommendation 26.*** *We recommend that the United States African Development Foundation's chief information security officer document and implement a process to provide annual role-based training to all personnel with significant information security responsibilities.*

~~**(SBU)**~~ In finalizing the report, Clifton evaluated USADF's responses to Recommendations 1 through 26 contained in the draft report. Both Clifton and OIG acknowledge USADF's management decisions for all 26 recommendations. However, we disagree with the decision for Recommendation 23. In their response, USADF officials did not state their intention to [redacted], which [redacted]. USADF [redacted], as required.[1] Therefore, we ask you to consider revising the management decision for Recommendation 23.

Thank you for your cooperation and the courtesies extended to our staff and Clifton's employees during the audit.

Sincerely,

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

[1] According to Federal Information Processing Standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004), systems are [redacted] Systems are [redacted]

CliftonLarsonAllen

USADF Lacks an Organization-Wide Information Security Program That Complies With FISMA

Final Report

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.claconnect.com

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 and 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 USAID 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 selected 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.

~~(SBU)~~ For this audit we reviewed the entire population of seven USADF information systems: the General Support System (GSS) and the Program Support System (PSS), [redacted]. The GSS is the framework network architecture that supports network security, Internet, and e-mail access. The PSS comprises applications that serve the USADF headquarters and the Foundation's constituents worldwide including the Grant Management Systems Database. USADF also uses five external information systems of shared services: [redacted]

[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 the Office of Management and Budget (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 and systems selected.

Results

The audit concluded that USADF did not implement its information security program in support of FISMA. USADF effectively implemented 41 of the 77 selected security controls. However, USADF did not effectively implement the remaining 36 controls in 12 areas tested.[3] Those 12 areas included:

- Program Management
- Security Assessment and Authorization
- Planning
- Risk Assessment
- System and Information Integrity
- Configuration Management
- Identification and Authentication
- Audit and Accountability
- Systems and Communication Protection
- System and Services Acquisition
- Awareness and Training
- Contingency Planning

~~(SBU)~~ To address its weaknesses in the above areas, USADF needs to:

- Strengthen its organization-wide information security program by appointing a Senior Agency Information Security Officer in accordance with FISMA and the National Institute of Standards and Technology (NIST).
- Perform security assessments and authorizations of systems in accordance with NIST standards and Office of Management and Budget (OMB) guidance.
- Update GSS, Office 365 and PSS security plans to comply with NIST Standards.
- Develop and fully implement a documented process to ensure that security assessments for the GSS, Office 365 and PSS are performed in accordance with NIST standards.
- Develop and fully implement a documented process to ensure that risk assessments for the GSS, Office 365 and PSS are performed and documented in accordance with NIST standards.
- Develop and fully implement a documented process to ensure that plan of action and milestones (POA&Ms) for the GSS and PSS include all known security control weaknesses, and are adequately documented, updated and managed.
- Develop and fully implement an entity-wide program for managing risk associated with the operation and use of the Foundation's information systems.
- Develop and fully implement a documented process to ensure the system inventory documentation is properly maintained.
- Develop and fully implement an enterprise architecture plan with consideration for information security and the resulting risk in accordance with NIST standards.

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

- Develop and fully implement a documented process to ensure [redacted], includes [redacted], and that [redacted] in accordance with USADF policy.
- Develop and fully implement a documented process to ensure configuration settings are monitored, any deviations are remediated timely and the component inventory is properly maintained.
- Develop and fully implement a documented process to ensure multifactor authentication is implemented and enforced for network access to privileged accounts. In addition, personal identity verification (PIV) credentials should be implemented and enforced for physical access to USADF facilities and local and network access.
- Develop and fully implement a documented process to ensure [redacted].
- Develop and fully implement a documented process to ensure all required audit events are logged, reviewed and analyzed in accordance with NIST requirements.
- Develop and fully implement a documented process to ensure the security categorization is reevaluated with consideration for personally identifiable information (PII) in accordance with OMB and NIST guidance for the GSS, [redacted].
- Develop and fully implement a documented process to ensure agreements with information system service providers are current.
- Develop and fully implement a documented process to ensure overseas partners complete annual security awareness training.
- Develop and fully implement a documented process to ensure contingency training and testing exercises are conducted in accordance with USADF's policy and contingency plan.

In 2014,[4] a security breach occurred on USADF's network and as a result of the above weaknesses, USADF's operations and assets have shown they are vulnerable to security breaches increasing the possibility of unauthorized access, misuse and disruption.

The weaknesses discussed in this report, specifically related to security assessment and authorization (SA&A) activities, were a result of USADF's ineffective risk management program. The SA&A activities at the information-system level, include documenting appropriate security controls in system security plans to protect information and information systems, testing and evaluating information security controls to ensure they were operating effectively, determining the associated risk, and authorizing information systems to operate were inadequately performed. This is a repeat issue that resulted in a significant deficiency to information system security in fiscal year 2015.

[4] United States Computer Emergency Readiness Team *Preliminary Digital Media Analysis Report (PDMAR) – INC000424776-C*, September 15, 2015.

Furthermore, USADF's risk management program is impacted by weaknesses noted this year related to vulnerability assessment, flaw remediation and configuration management. The lack of an effective risk management program represents a significant deficiency to information system security again for the 2016 FISMA assessment. According to OMB, a significant deficiency is:

> A weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and other agencies must be notified and immediate or near-immediate corrective action must be taken.[5]

We are making 26 recommendations to assist USADF in establishing and maintaining an effective information security program. Considering the volume of internal control weaknesses identified, USADF needs to appoint in writing a Senior Agency Information Security Officer in accordance with requirements prescribed by the Federal Information Security Modernization Act of 2014 and the National Institute of Standards and Technology. In addition, USADF needs to develop and implement detailed POA&Ms to implement an organization-wide information security program in accordance with FISMA and NIST requirements. At a minimum, those POA&Ms must address the 26 recommendations identified in this report.

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

In response to the draft report, USADF outlined and described its plans to address all 26 audit recommendations. Based on our evaluation of management's comments, we acknowledge USADF's management decisions on all 26 recommendations. However, we do not agree with the management decision on Recommendation 23 and respectfully request USADF to revise it. USADF's comments are included in their entirety in Appendix II.

[5] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (November 18, 2013).

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,* 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 has not properly implemented an organization-wide information security program. Specifically, weaknesses were noted in the following program management controls tested:

- Senior Information Security Officer
- Security Authorization Process
- Plan of Action and Milestones Process
- Risk Management Strategy
- Information System Inventory
- Enterprise Architecture

Senior Information Security Officer

FISMA requires agencies to appoint a Senior Information Security Officer with information security duties as that individual's main responsibility. Typically agencies refer to this individual as the Chief Information Security Officer (CISO).

FISMA states:

> § 3554. Federal agency responsibilities
> ''(a) IN GENERAL.—The head of each agency shall—
> …
> ''(3) delegate to the agency Chief Information Officer established
> under section 3506 (or comparable official in an agency
> not covered by such section) the authority to ensure compliance
> with the requirements imposed on the agency under this subchapter,
> including—
> ''(A) designating a senior agency information security
> officer who shall—
> ''(i) carry out the Chief Information Officer's
> responsibilities under this section;
> ''(ii) possess professional qualifications, including
> training and experience, required to administer the
> functions described under this section;

> ‘‘(iii) have information security duties as that official’s
> primary duty; and
> ‘‘(iv) head an office with the mission and resources
> to assist in ensuring agency compliance with this section;

NIST SP 800-53, Revision 4, security control PM-2, states:

> The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
>
> *Supplemental Guidance*: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

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

> The USADF CIO shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an enterprise-wide information security program.

USADF did not appoint a senior information security officer to coordinate, develop, implement, and maintain an information security program in accordance with FISMA and NIST requirements. USADF assigned both the CIO and CISO functions to an individual who was not a senior officer. This individual reports to the Chief Financial Officer. Management indicated that due to the size of the foundation and resulting budget for information technology and security resources, appointing a senior information security officer with information security and compliance as that individual’s primary duty was not feasible. By not appointing a senior official as the CISO, the importance of information security was weakened and has resulted in the lack of adequate resources.

In addition since the individual assigned to perform the CISO’s functions also performs the CIO’s functions, he is responsible for both information technology (IT) operations and compliance. This creates a segregation of duties issue because the CISO is responsible for ensuring IT operations that he oversees are compliant with FISMA. With the CISO’s responsibilities not being independent from the IT operation’s function, the ability to independently and effectively assess compliance with security requirements was diminished. This may result in increased risk that the foundation will not have security protections in place commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems as discussed in the other findings in this report.

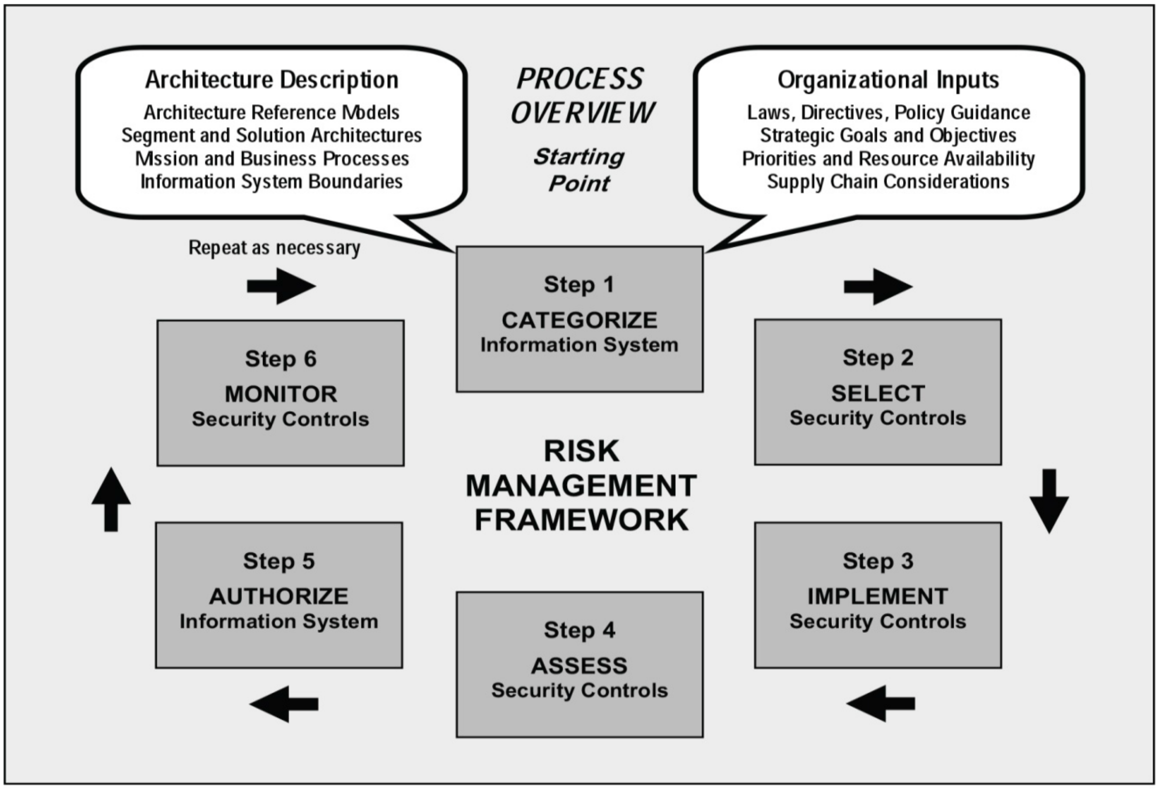
> ***Recommendation 1:*** *We recommend that the United States African Development Foundation’s President appoint in writing a senior-level Chief Information Security Officer in accordance with the Federal Information Security Modernization Act and the National Institute of Standards and Technology.*

Security Authorization Process

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 system security plan; 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 Special Publication (SP) 800-37 Rev. 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 Figure 1 below:

Figure 1: NIST Risk Management Framework


Architecture Description
Architecture Reference Mbdels
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 Special Publication (SP) 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

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 ;

In addition, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 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. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the authorization package. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization ensures that the information needed for authorizing officials to make risk based decisions, is made available by the provider.

Furthermore, the *USADF Information Technology Security Implementation Plan,* states:

> The USADF CISO shall ensure that:
>
> - The security state of USADF information systems is managed (i.e., documents, tracks, and reports) through security authorization processes;
> - Individuals to fulfill specific roles and responsibilities within the USADF risk management process are designated; and
> - The security authorization process is fully integrated into an enterprise-wide risk management program.

To address five prior year recommendations related to security assessment and authorization activities,[6] USADF procured a contractor to assist with the security authorization packages for the two cloud-based systems, PSS and Office 365. In addition, USADF issued an authorization to operate (ATO) on August 31, 2015, for the PSS and an ATO on April 18, 2016, for Office 365. However, USADF did not follow NIST requirements throughout the security assessment and authorization process. Specifically, issues were identified with the system security plans, the security control assessments, and the risk assessments as discussed in the following section.

<u>System Security Plans</u>

The purpose of a system security plan (SSP) is to describe the information system, including the system boundary and document the security controls both planned and implemented for the system.

[6] 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).

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

> 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

The *USADF Information Technology Security Implementation Plan,* states:

> Each SSP must contain, at a minimum, the following information:
>
> - Defined system authorization boundary;
> - Description of the security controls in place or planned for meeting those requirements including a decision rational for tailoring and supplementation of controls.
>
> For all USADF information systems, the SSP must be updated annually or when a major system change occurs, whichever comes first. Major changes include, but are not limited to, the information system operation, architecture environment, or problems identified during plan implementation or security control assessment.

The PSS, Office 365 and GSS system security plans were not documented in accordance with NIST requirements. For example, the system security plans were incomplete and/or did not reflect the current operating environment. Specifically:

- The PSS SSP 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.
- The Office 365 SSP stated that USADF did not have specific policies and procedures to address each control family. However, USADF had documented policies and procedures in the *USADF Information Technology Security Implementation Plan* for each control family. The SSP also stated that organization defined parameters were inherited from the Federal Risk and Authorization Management Program[7] Office 365 package. However, the *USADF Information Technology Security Implementation Plan* documented the organization defined parameters as required by USADF. In addition, the control implementation descriptions were not completely documented for 12 of the 134 controls.

[7] The Federal Risk and Authorization Management Program is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

- The GSS SSP stated that USADF conducted the last annual control assessment in April of 2011. However the last annual assessment was performed in 2013. In addition, the POA&M process referenced a POA&M report from 2014. Based on review of the POA&M report, the most recent POA&Ms were from 2015. In addition, the information regarding outsourced Information System Services did not include the cloud service providers. Furthermore, the SSP stated that USADF was in the process of developing a formal security measure of performance document; however, security measures of performance were implemented with USADF's continuous monitoring program. Moreover, the control implementation descriptions were not completely documented for 26 of the 170 controls. A recommendation to review and update the GSS's system security plan on an annual basis to include a determination of whether the security requirements and controls for the system are adequately documented and reflect the current information system environment was made in the fiscal year 2015 audit.[8] USADF did not take final action to close this recommendation.

Additionally, the control implementation descriptions were not documented for the privacy controls specified in NIST SP 800-53, Revision 4, Appendix J, for the PSS, Office 365 or GSS System Security Plans. A recommendation to update the GSS's security plan to reflect privacy controls was made in the fiscal year 2015 audit.[9] USADF closed the recommendation, though corrective action was not taken.

This occurred because the individual assigned to perform CISO functions did not monitor the work performed by the contractor to ensure the security requirements and controls for the system were adequately documented and reflected the current information system environment. Without complete and up-to-date system security plans, USADF systems could be susceptible to unknown security risks resulting from changes to the environment.

Because USADF officially closed the recommendation from our fiscal year 2015 audit report[10] and the weaknesses noted this year included PSS, Office 365 and the GSS, we are issuing a new recommendation to correct the weaknesses observed related to system security plans for all USADF systems.

> ***Recommendation 2:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and fully implement a documented 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 should include a determination whether the security requirements and controls for the system are adequately documented and reflect the current information system environment.*

[8] 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).

[9] Recommendation 2, *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).

[10] Ibid. footnote 9.

Security Control Assessments

After documenting the controls in place or planned in the system security plan, NIST requires that information system security controls be evaluated during the risk assessment process to determine whether controls are operating properly and as intended.

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

> The organization:
>
> a. Develops a security assessment plan that describes the scope of the assessment including:
>   1. Security controls and control enhancements under assessment;
>   2. Assessment procedures to be used to determine security control effectiveness; and
>   3. Assessment environment, assessment team, and assessment roles and responsibilities;
>
> 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 ;

The *USADF Information Technology Security Implementation Plan* states:

> USADF shall conduct an assessment of the security controls in accordance with the OMB policy to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.
>
> 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.

The security control assessments performed for the PSS and Office 365 systems were not conducted in accordance with NIST requirements. Specifically, a security test plan was not documented with detailed test procedures. In addition, a test of whether the controls were implemented and operating as intended was not performed for all controls assessed for the PSS and Office 365 security control assessments. Further, the individual assigned to perform CISO functions did not provide adequate oversight of the contractor performing the security assessments to ensure they were performed in accordance with NIST standards. This would have included documented plans that describe procedures to be used to determine security control effectiveness and testing the operating effectives of security controls.

In addition, a security control assessment for the GSS was not conducted annually as required by USADF policy. The last assessment performed was in 2013. The individual assigned to perform CISO functions thought that by testing controls for Active Directory during the Office 365 assessment, the GSS was tested. However, the GSS components housed, operated and maintained by USADF were not tested.

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

A recommendation to ensure that a security assessment is conducted annually for the General Support System as required by USADF policy[11] and a recommendation to ensure that security assessment plans are documented for the General Support System that describe the scope of the assessment and assessment procedures to be used to determine security control effectiveness as required by NIST[12] were made in the fiscal year 2015 audit. Management did not officially closed those recommendations, however since the weaknesses noted this year included PSS, Office 365 and the GSS, we are issuing a recommendation to correct the weaknesses related to security control assessments for all USADF systems.

> ***Recommendation 3:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to perform security assessments in accordance with National Institute of Standards and Technology standards. This includes documented plans that describe assessment procedures to be used to determine security control effectiveness and testing the operating effectiveness of security controls.*

Risk Assessments

Upon completion of the security control assessment a risk assessment is performed to identify risks to the foundation pertaining to the operation of USADF's information systems. When assessing risk, an analysis of known threats and vulnerabilities should be considered.

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 ;
>
> *Supplemental guidance*: Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets,

[11] Recommendation 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).

[12] Recommendation 4, *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).

> individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).

The *USADF Information Technology Security Implementation Plan*, states:

> The risk assessment shall determine the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information system.
>
> 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).

The risk assessments for the PSS, Office 365 and GSS did not take into account all known risks. Specifically:

- The PSS risk assessment did not include information regarding the system being hosted by a cloud-based service provider or an analysis of the inherited risks.
- Although the Office 365 risk assessment addressed the transition of the system to a cloud-service provider, it did not include an analysis of the inherited risks.
- None of the control weaknesses that were noted in the PSS and Office 365 security control assessments were addressed in the risk assessments.
- None of the controls noted as planned in the PSS and Office 365 system security plans were documented and analyzed in the risk assessments.

  The risk assessment results identified in the GSS risk assessment were outdated. They reflected the results of the last security control assessment conducted in 2013. In addition, the 4 open GSS POA&Ms were not included in the risk assessment. Furthermore 6 of the 7 planned controls in the GSS system security plan were not addressed in the risk assessment.

In addition to a lack of oversight to ensure the system security plans and security control assessments met NIST requirements, the individual assigned to perform CISO functions did not monitor the contractor to ensure the risk assessments took into account all known risks including the risks associated with the use of cloud-service providers. In order to meet a scheduled deadline, this individual certified to the authorizing official that the systems met the documented security requirements and recommended the systems be authorized to operate. Based on that recommendation, the authorizing official authorized the systems to operate even though the security controls were not adequately documented and assessed, and a risk assessment was not properly performed and documented.

The lack of adequately documented risk assessments increases the risk that the Authorizing Official does 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.

> ***Recommendation 4:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process for 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. This includes an analysis of the associated risks inherited from cloud-service providers.*

Plan of Action and Milestone Process

POA&Ms describe corrective action plans for system weaknesses noted from security control assessments, vulnerability assessments and system audits. The POA&Ms are used by the authorizing official to monitor the progress of remediation for system control weaknesses.

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

Also NIST SP 800-53, Revision 4, security control CA-5, states the following regarding POA&Ms:

> The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

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.
- The POA&M will document planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities in the system.
- USADF system POA&Ms shall be updated periodically, at least quarterly. All deficiencies (ongoing, completed and delayed) for the quarter shall be reported as required.

USADF's POA&M management process had weaknesses for the PSS, Office 365 and GSS systems. Specifically, the POA&Ms did not include all known weaknesses and the documentation was incomplete. For example:

- Thirty-nine controls of the 45 planned controls listed in the PSS SSP were not included in the POA&Ms. In addition, planned corrective actions were not documented for the entire population of seven PSS POA&Ms, and the estimated completion date was not documented for five of them.
- The entire population of five planned controls listed in the Office 365 SSP, were not included in the POA&Ms.
- Six of the total population of seven planned controls in the GSS SSP were not included in the POA&Ms. In addition, planned corrective actions were not documented for six of the eight GSS POA&Ms. Furthermore, two POA&Ms with scheduled completion dates of September 30, 2014 were not closed and a justification for missing the scheduled completion date and a new estimated completion date were not documented.

In addition, the control weaknesses noted in the FY 2015 FISMA audit were not included in the POA&Ms. Furthermore, milestone information was not updated on a quarterly basis as required by USADF policy for the entire population of seven PSS and nine GSS POA&Ms.

The individual assigned to perform CISO functions did not place the proper amount of attention on documenting and updating 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 and associated corrective action plans and are updated quarterly as required by USADF policy.

Without documenting and tracking all known system security control weaknesses and associated corrective actions and in the POA&Ms, USADF remains susceptible to system security risks. Furthermore, not updating POA&Ms to reflect their current status affects USADF's ability to effectively manage system security risks associated with their systems.

> ***Recommendation 5****: We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to include all known security weaknesses and associated corrective plans in the plan of action and milestones, and to update them quarterly as required by the foundation's policy.*

Risk Management Strategy

NIST requires organizations to develop an entity-wide program for managing risk associated with the operation and use of the agency's information systems.

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

> The USADF CISO shall develop and implement a comprehensive strategy to manage risk to USADF's operations and assets, individuals, other organizations and the Nation associated with the operation and use of information systems.

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. Management indicated that developing an organization-wide risk management program was important but senior leaders had not yet coordinated the effort to develop, document and implement an entity-wide risk management 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.

> ***Recommendation 6:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented 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.*

Information System Inventory

FISMA requires each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of — (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Identifying, documenting and maintaining an accurate inventory of an agency's information systems is key for ensuring adequate security protections are implemented.

NIST SP 800-53, Revision 4, security control PM-5, states, "The organization develops and maintains an inventory of its information systems."

The *USADF Information Technology Security Implementation Plan*, states, "The USADF CISO shall ensure that an inventory of all USADF information systems is developed and maintained up to date."

The information system inventory was not up-to-date and accurately described. The USADF system inventory information documented in the *Security Classification and Rating* documentation was last updated in 2014. This was before USADF completed its transition to the Microsoft Office 365 cloud system and to an Amazon hosted cloud based system for the Program Support System. Therefore the inventory did not reflect the transition to cloud based systems, including the identification of Federal Risk and Authorization Management Program [13] approval status.

The individual assigned to perform CISO functions did not ensure the system inventory documentation was properly maintained by periodically reviewing and updating the details. Without an up-to-date and accurate inventory description of USADF's information systems, there is an increased risk that security controls will not be appropriately implemented for all USADF systems to strengthen protection from unauthorized access, viruses, malicious code, and exploitable vulnerabilities.

> ***Recommendation 7:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to review and maintain up-to-date information system inventory documentation.*

[13] The Federal Risk and Authorization Management Program is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

Enterprise Architecture

To effectively achieve an agency's mission the information technology that supports the agency's operations should be strategically planned and implemented. NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View* states:

> A well-designed enterprise architecture implemented organization-wide, promotes more efficient, cost-effective, consistent, and interoperable information security capabilities to help organizations better protect missions and business functions—and ultimately more effectively manage risk.

NIST SP 800-53, Revision 4, security control PM-7, states the following regarding enterprise architecture:

> The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
>
> *Supplemental Guidance*: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems.

In addition, the USADF *Information Technology Security Implementation Plan* states, "The USADF CISO shall develop and maintain an enterprise architecture and ensure that the enterprise architecture integrates information security."

USADF did not have a process in place to document an enterprise architecture plan with consideration for information security and the resulting risk. The individual assigned to perform CISO functions believed that a documented enterprise architecture was not necessary for USADF given the size of the foundation and the simplicity of its information technology environment.

Without developing and documenting an enterprise architecture, USADF may not be efficiently, cost-effectively, and consistently applying adequate protections to enable the foundation to successfully meet its mission through its business functions and effectively manage risk.

> ***Recommendation 8:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to develop, document and implement an enterprise architecture in accordance with National Institute of Standards and Technology standards.*

2. ~~(SBU)~~ [redacted] Needs Strengthening

~~(SBU)~~ NIST requires organizations to [redacted] their information systems for [redacted] and [redacted] within a specified timeframe. [redacted] includes scanning for [redacted].

~~(SBU)~~ NIST SP 800-53, Revision 4, security control [redacted] states the following regarding [redacted]:

> ~~(SBU)~~ The organization:
>
> [redacted]

~~(SBU)~~ Security control [redacted] states the following regarding [redacted]:

> The organization:
>
> [redacted]

~~(SBU)~~ The USADF *Information Technology Security Implementation Plan,* [redacted] states:

> [redacted]
>
> 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.

In addition, the USADF *Information Technology Security Implementation Plan*, SI-2 states:

> To ensure that the USADF's computing environment is safe, USADF's IT security staff regularly push out security updates to workstations, and laptops assigned to USADF staff.

Also, *USADF Patch Management Procedures* state:

> For normal security updates, schedule a push as prescribed in the USADF Patch Management and Remediation policy.
>
> For security patches recommended by the United States Computer Emergency Readiness Team (US-CERT), schedule a test every Tuesday for the following system:
>
> a. ADF laptops and desktops (Windows 7 & Office 2010)
> b. ADF laptops and desktops (Approved software vendors other than Microsoft)
> c. ADF Servers
>
> Send out a notice to USADF users notifying them of new security patches on Wednesday if testing was successful.

~~(SBU)~~ Weaknesses were noted with [redacted]. Specifically, USADF's [redacted] in accordance with USADF policy. In addition, USADF did not [redacted] in accordance with USADF policy and did not [redacted]. For example:

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

~~(SBU)~~ The individual assigned to perform CISO functions did not fully [redacted]. In addition, he did not provide satisfactory supervision to ensure that [redacted] in accordance with USADF policy. Furthermore, this individual did not implement a process to [redacted] Moreover, documented acceptance and approval of risk, including adequate compensating controls related to [redacted] was not performed. Overall, [redacted] was not given the proper priority in the configuration management process.

~~(SBU)~~ Without complete [redacted] These weaknesses [redacted] in USADF's [redacted]. In addition, not [redacted] may provide [redacted] Furthermore, [redacted].

> ~~(SBU)~~ ***Recommendation 9***: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to perform* [redacted].

~~(SBU)~~ ***Recommendation 10:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a documented process to* [redacted] *in accordance with the foundation's policy. This includes ascertaining* [redacted] *in accordance with policy.*

Recommendation 11: *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. Configuration Management Controls Need Strengthening

NIST defines configuration management as a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

NIST SP 800-53, Revision 4, security control CM-6, states the following regarding configuration settings:

> The organization:
>
> a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
> b. Implements the configuration settings;
> c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and
> d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

The *USADF Information Technology Security Implementation Plan*, CM-6 states:

> Configuration Managers and System Administrators, in conjunction with ISSOs, shall apply the appropriate Security Technical Implementation Guide (STIG) and maintain the established configuration for information systems under their control.
>
> For USADF systems, detection of unauthorized, security-related configuration changes shall be incorporated into the USADF's incident response capability for

> the purpose of tracking, monitoring, correction and availability.

In order to effectively manage the configuration of the foundation's systems, accurate accountability of information system component inventories is required.

NIST SP 800-53, Revision 4, security control CM-8, states the following regarding the information system component inventory:

> The organization:
>
> a. Develops and documents an inventory of information system components that:
>   1. Accurately reflects the current information system;
>   2. Includes all components within the authorization boundary of the information system;
>   3. Is at the level of granularity deemed necessary for tracking and reporting; and
>   4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
>
> b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

The *USADF Information Technology Security Implementation Plan*, CM-8 states:

> For all USADF information systems and applications, the system owner or designated representative shall develop, document and maintain a current inventory of all information systems' components.

The following weaknesses were identified pertaining to configuration settings and inventory component management.

~~(SBU)~~ Regarding configuration settings:

- USADF did not [redacted] USADF did not [redacted]. Instead, USADF only reviewed the [redacted]. In addition, several users were [redacted] thereby allowing [redacted]. Therefore [redacted] would have to be reviewed to [redacted]. Management did not document compensating controls and formally accept the risk of allowing [redacted]. Without [redacted] These weaknesses expose gaps in USADF's [redacted].
- USADF did not [redacted] The individual assigned to perform CISO functions did not

provide adequate supervision of personnel to ensure [redacted] documented and approved thereby increasing the risk that employees are [redacted].

- The [redacted] was not [redacted] in accordance with USADF policy. The [redacted] was [redacted]; however, USADF policy required [redacted]. The individual assigned to perform CISO functions did not ensure the [redacted]. Failure to [redacted] in accordance with the foundation's policy increases the risk of unauthorized access potentially leading to unauthorized modification, loss or disclosure of USADF information.
- [redacted] did not require [redacted]. Without [redacted] can be [redacted] by an unauthorized user to gain access to USADF information systems. Upon notification of this issue to the individual assigned to perform CISO functions, he determined these were [redacted]. He subsequently stated the [redacted]. When [redacted] the risk is increased that [redacted], making the [redacted] providing access to sensitive data.

~~(SBU)~~ Concerning [redacted], USADF policy did not specify a frequency to review and update the [redacted]. The individual assigned to perform CISO functions stated that the [redacted] was not performed. Based on review of the [redacted], the [redacted] either in 2012 or 2014. If the [redacted] had been reviewed and updated, the likelihood is increased that the [redacted] above would have been [redacted].

~~(SBU)~~ The individual assigned to perform CISO functions did not provide acceptable attention to detail in [redacted] the policy specified the [redacted] requirement. In addition, the CISO did not adequately supervise the personnel responsible for completing the [redacted] to ensure the task was performed as required. The lack of [redacted] increases the risk that security controls may not be implemented for [redacted] exposing USADF information to unauthorized modification, loss, and disclosure.

> ~~(SBU)~~ ***Recommendation 12:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to* [redacted] *including* [redacted].

> ~~(SBU)~~ ***Recommendation 13:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to* [redacted] *to foundation*

[redacted] *and to* [redacted]. *That process must include formally documenting the risk and granting approval, including adequate compensating controls, if an exception must be made.*

Recommendation 14*: We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to document, approve and disseminate approved deviations from United States Government Configuration Baseline settings.*

Recommendation 15: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement written a process to configure password settings in accordance with the foundation's policy. This process must include monitoring the password settings on the foundation's information systems on an ongoing basis. In addition passwords should be encrypted during authentication.*

Recommendation 16: *We recommend that the United States African Development Foundation's Information Security Officer develop and implement a written process to specify an organization-defined frequency to review and update the information system component inventory.*

Recommendation 17: *We recommend that the United States African Development Foundation's Information Security Officer develop and implement a written process to maintain the inventory according to policy.*

Recommendation 18: *We recommend that the United States African Development Foundation's Information Security Officer develop and implement a written process to remove and decommission unused systems timely.*

4. Identification and Authentication Controls Need Strengthening

NIST requires information systems to uniquely identify and authenticate users and devices prior to granting access. However, issues were identified related to the following controls:

- Multifactor authentication for privileged and non-privileged users ; and
- Default Authenticators

Multifactor Authentication

Multifactor authentication requires users to authenticate with additional credentials other than solely a user name and password. Examples of additional credentials are a token or Personal Identity Verification (PIV) credentials issued by federal agencies. NIST requires all federal information systems to require multifactor authentication for network access to privileged accounts and the use of PIV.

NIST SP 800-53, Revision 4, security control IA-2, control enhancement (1) states, "The information system implements multifactor authentication for network access to privileged accounts."

The *USADF Information Technology Security Implementation Plan*, IA-2 states, "All USADF information systems must employ multi-factor authentication for network access to privileged accounts."

In addition, 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, Rev 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.

In addition, the *USADF Information Technology Security Implementation Plan*, IA-2 states:

> If a Personal Identification Verification card or token is used, it must be conformed to the specifications in FIPS 201 Personal Identity Verification for Federal Employees and Contractors, NIST SP 800-73 Interfaces for Personal Identity Verification, and NIST SP 800-76 Biometric Data Specifications for Personal Identity Verification.

USADF did not implement multifactor authentication for network access to privileged accounts. In addition, PIV credentials were not implemented for physical access to USADF facilities for personnel, and local and network access for non-privileged accounts. The *USADF Information Technology Security Implementation Plan* does not require the use of PIV credentials. The individual assigned to perform CISO functions specified that the foundation had obtained the PIV cards but did not have the guidance and tools to implement the technology. USADF has a current POA&M with a scheduled completion date of December 31, 2016.

Without multifactor authentication for network access to privileged accounts there is an increased risk of unauthorized access by an unauthorized user. Unauthorized privileged access can allow an individual to inappropriately create, delete and modify users and services running on the network as well as gain access to all data stored on the network.

In addition without implementing and enforcing multifactor authentication for physical access to USADF facilities and for non-privileged user accounts there is increased risk of unauthorized access to USADF information and information systems by an unauthorized user decreasing the confidentiality and integrity of data.

Recommendation 19: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to implement and enforce multifactor authentication network access to privileged accounts.*

Recommendation 20: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to implement and enforce Personal Identity Verification credentials for physical access to the foundation's facilities and local and network access.*

~~(SBU)~~ [redacted]

~~(SBU)~~ [redacted].

~~(SBU)~~ NIST SP 800-53, Revision 4, security control [redacted] states:

> The organization [redacted]
> …
> [redacted]

~~(SBU)~~ The *USADF Information Technology Security Implementation Plan*, [redacted] states:

> [redacted]
>
> - [redacted].

~~(SBU)~~ [redacted] The individual assigned to perform CISO functions did not carefully oversee [redacted]. In addition, this [redacted] was not detected and remediated by USADF.

~~(SBU)~~ [redacted] Therefore, USADF's information and information systems are at increased risk of unapproved access and changes.

~~(SBU)~~ ***Recommendation 21:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to* [redacted].

5. Review and Analysis of Audit Logs Needs Strengthening

NIST requires information systems to audit events deemed significant to the security of the information system and the environment in which those systems operate. In addition, the audit events must be reviewed, analyzed and reported in order to respond to and remediate incidents timely.

NIST SP 800-53, Revision 4, security control AU-2 states the following regarding audit events:

> The organization:
>
> a. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]."

Control AU-3 states,

> The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control AU-6 states the following regarding audit review, analysis and reporting:

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

Control SC-7 states the following regarding boundary protection:

> The information system:
>
> a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system ;

The USADF *Information Technology Security Implementation Plan*, AU-2 states, "All USADF information systems will be configured to generate and collect audit records."

AU-6 states:

> For all USADF information systems, System Administrators will review and analyze audit records on a daily basis for indications of any unusual or inappropriate activity. All suspicious activities shall be investigated and reported to the System Owner and CISO as required by the Incident Response Policy in a prompt manner.

SC-7 states:

> For all USADF systems that connect to the Internet, networks external to USADF, and at key internal boundaries within the system, the System Owner, in conjunction with the CISO and network and System Administrators, shall establish the use of boundary protection devices, such as proxies, gateways, routers, firewalls, and/or encrypted tunnels.

The following issues were noted related to logging of audit events and review and analysis of audit logs:

- Management did not provide evidence that firewall events were logged, reviewed and analyzed.
- Although network events were logged, management did not provide evidence that the events were reviewed and analyzed.
- Although remote access activity was logged, management did not provide evidence that the activity logs were reviewed and analyzed.

The individual assigned to perform CISO functions was not able to access the firewall event log report. In addition, this individual did not ensure evidence was retained to validate that the network event logs and remote access activity logs were reviewed. Without monitoring audit logs, unauthorized individuals may gain system access and conduct malicious activities without detection.

> ***Recommendation 22:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to review and analyze all required audit events in accordance with National Institute of Standards and Technology standards and the foundation's policy.*

6. Information System Categorization Process Needs Strengthening

The first step in the NIST RMF process is to categorize information systems to analyze and document the adverse impacts should the agencies information and information systems become compromised through a loss of confidentiality, integrity or availability.

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

> The organization:
>
> a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance ;

OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* states:

> Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* states:

> PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
>
> To distinguish an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data. In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.
>
> The following list contains examples of information that may be considered PII.
>
> - Name, such as full name, maiden name, mother‘s maiden name, or alias
> - Address information, such as street address or email address
> - Telephone numbers, including mobile, business, and personal numbers

~~(SBU)~~ The [redacted]contain personally identifiable information (PII); however, they were [redacted] systems. Management stated that [redacted] contains documents with only employee names and phone numbers which they did not consider PII, and therefore [redacted]. According to NIST’s definition of PII, the GSS should have been categorized at a minimum as a moderate system since employee names and phone numbers are stored on the system.

~~(SBU)~~ In addition, management indicated that the [redacted] are external systems owned and operated by other federal agencies. Since those agencies are responsible for the systems’ security controls, management [redacted] by those external agencies as documented in the Interagency Security Agreements. However, since the systems contain PII, USADF should have [redacted] the systems at a minimum as [redacted] systems in order to ensure controls that USADF ha [redacted].

~~(SBU)~~ Without designating the proper [redacted] to the foundation’s information systems, USADF is at increased risk that effective security controls are not in place for these systems. USADF may be exposed to inappropriate or unauthorized access to PII which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

~~(SBU)~~ ***Recommendation 23:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to* [redacted] *with consideration for* [redacted] *in accordance with the Office of Management and Budget and National Institute of Standards and Technology guidance.*

7. External Information System Agreements Need to be Current

When agencies use systems owned and operated by external parties it is necessary to ensure that external service providers employ adequate security controls in order to protect the agency's data. A Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) document the agreement governing the interconnection to the third parties information system.

NIST SP 800-53, Revision 4, security control SA-9, states the following regarding external information system services:

> The organization:
>
> a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
> b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
> c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* states:

> The participating organizations perform preliminary activities; examine all relevant technical, security, and administrative issues; and form an agreement governing the management, operation, and use of the interconnection.
>
> The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team's review of all relevant technical, security, and administrative issues.
>
> The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection.
>
> The MOU/A documents the terms and conditions for sharing data and information resources in a secure manner.

The ISA and MOU between USADF and the Department of Interior (DOI) Interior Business Center (IBC) expired on January 4, 2016. This agreement addresses the interconnections between the two party's networks for the purpose of providing USADF users access to the IBC Payroll and Human Resources systems and the connections within the USADF network utilizing service accounts to transfer data through the system-level interfaces. The individual assigned to perform CISO functions was working with DOI to execute an updated agreement; however, at the time of testing DOI had not sent USADF the prepared agreement for review and approval.

Without an agreement, security controls that will be in place to protect the confidentiality, integrity, and availability of the DOI/IBC and USADF systems and the data transferred between them are not documented increasing the risk that adequate security of USADF data will not be implemented. In addition, when system interfaces are not accurately understood and documented there is an increased risk that data may be added, lost or altered during processing.

> ***Recommendation 24:*** *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to maintain a current Interconnection Security Agreement and Memorandum of Understanding between the foundation and Department of Interior's Interior Business Center.*

8. Security Awareness and Training Needs Strengthening

NIST requires organizations to provide personnel and contractors with fundamental knowledge regarding information security and security incident responsibilities.

Security Awareness Training

NIST SP 800-53, Revision 4, security control AT-2, states the following regarding security awareness training:

> The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
>
> a. As part of initial training for new users;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

The USADF *Information Technology Security Implementation Plan*, AT-2 states:

> All USADF information system users including contractors, volunteers, managers and senior executives shall take USADF-provided information system security awareness training prior to accessing USADF information systems and at least annually thereafter.

Not all USADF system users completed annual security awareness training. Due to Internet bandwidth limits, overseas partners did not complete the online training course. As a result, 12 individuals who were overseas partners from a sample of 17 PSS users did not complete annual security awareness training. The individual assigned to perform CISO functions did not make available an alternative method for overseas partners to complete annual security awareness training.

Without periodic security awareness training employees may be more likely to inadvertently perform unsafe practices such as using weak passwords or sharing passwords, responding to phishing emails, or introducing malware to the foundation's systems. These practices increase risk to USADF's information and information systems.

Role-Based Security Training

NIST also requires personnel with significant information system security responsibilities to complete role-based security training.

Security control AT-3, states the following regarding role-based security training:

> The organization provides role-based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

The USADF *Information Technology Security Implementation Plan*, AT-3 states:

> All personnel assigned significant information security roles shall take information security training commensurate with their responsibilities and system requirements before receiving access to systems, when required as a result of system changes, and annually thereafter.

One of two users sampled with significant information security responsibilities did not complete annual role-based security training. The individual assigned to perform CISO functions did not monitor to ensure role-based training was completed. Without specialized training, individuals responsible for system administration and security of USADF information systems may not maintain the knowledge required to perform their responsibilities. Personnel may be performing tasks without proper training, thus potentially increasing the risk that the foundation's information and information system could become compromised leading to unauthorized access, data loss, data manipulation and unavailability.

Recommendation 25: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to provide annual security awareness training to overseas partners.*

Recommendation 26: *We recommend that the United States African Development Foundation's Chief Information Security Officer develop and implement a written process to provide annual role based training to all personnel with significant information security responsibilities.*

9. Contingency Planning Training and Testing Needs Strengthening

NIST requires organizations to train employees on contingency activities and test their contingency plans at a specified frequency to determine effectiveness of the plan.

NIST SP 800-53, Revision 4, security control CP-3, states the following regarding contingency training:

> The organization provides contingency training to information system users consistent with assigned roles and responsibilities :
>
> a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

Security control CP-4, states the following regarding contingency testing:

> The organization:
>
> a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
> b. Reviews the contingency plan test results; and
> c. Initiates corrective actions, if needed.

The USADF *Information Technology Security Implementation Plan*, CP-4 states:

> Personnel involved in executing the contingency plan shall receive annual training in their contingency roles and responsibilities with respect to the information systems.
>
> The contingency plan coordinator shall be responsible for conducting annual contingency plan training, which may coincide with contingency plan testing.

CP-4 states, “USADF contingency plan shall be tested annually for mission critical systems that are hosted within USADF HQ Data Center.”

According to the *USADF Information Technology Contingency Plan*, the plan is to be reviewed and tested annually. Part of the IT contingency testing includes testing of infrastructure components in the data center that provide support for the IT infrastructure.

In the fiscal year 2015 audit, a recommendation was made to ensure that the contingency plan for the General Support System and Program Support System is tested to ensure personnel are trained on how to respond in the event of a disruption of cloud-based services.[14]

USADF did not conduct contingency planning training and testing exercises for the information system components hosted within the USADF data center to verify its effectiveness. The individual assigned to perform CISO functions did not provide oversight to ensure that the contingency plan was tested on an annual basis. Without providing contingency training and testing the recovery capability of their systems, USADF is at risk of a successful restoration in the event of a disaster.

Since management did not close this recommendation, an additional recommendation is not made at this time.

[14] Recommendation 11, *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).

EVALUATION OF MANAGEMENT COMMENTS

In response to the final report, the United States African Development Foundation (USADF) outlined its plans to address all 26 recommendations and described planned actions to address the recommendations. USADF's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on recommendations 1 through 26, though we disagree with the decision for Recommendation 23.

~~(SBU)~~ In response to Recommendation 23, USADF agreed to document and implement a process to [redacted] in accordance with OMB Memorandum 07-16 and NIST SP 800-21 and plans to complete that action August 31, 2017. In regard to its [redacted], USADF commented that it will make efforts to obtain the [redacted] from the system owners [redacted] and [redacted]. However, USADF is responsible for certain controls, such as [redacted] and ensuring these controls are adequately addressed and implemented. As such, USADF should assess and document the risk the [redacted] pose to USADF and categorize the systems in accordance with FIPS 199, taking into account that the systems [redacted]. Therefore, we respectfully request USADF to revise its management decision for Recommendation 23 to specifically include a written process to [redacted] of its [redacted].

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 United States African Development Foundation (USADF) implement selected security controls for selected information systems[15] in support of the Federal Information Security Modernization Act of 2014.

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.* 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
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

For this audit we reviewed the entire population of seven USADF information systems: the General Support System, the Program Support System, Payroll, Human Resources, PRISM, Oracle Financials, and Travel. See Appendix III for a listing of selected controls for each system. 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. In addition, the audit included a follow up

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

on prior year audit recommendations[16] 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 3, 2016, through July 7, 2016.

Methodology

Following the framework for minimum security controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, certain controls (listed in Appendix III) were selected from NIST security control families.[17] We reviewed the selected controls[18] over USADF's General Support System, Program Support System, Payroll, Human Resources, PRISM, Oracle Financials, and Travel.

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, 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 USADF's general support system and evaluated USADF's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of USADF vulnerability scanning configurations and network vulnerability scan results and comparing them with independent network vulnerability scan results.
- Reviewed the status of recommendations in the fiscal year 2015 FISMA audit report, including supporting documentation to ascertain whether the actions taken addressed the weakness.[19]

In testing for the adequacy and 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

[16] *Audit of the U.S. African Development Foundation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, as amended* (Audit Report No. A-ADF-16-002-P, November 13, 2015).

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

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

[19] *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).

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.

MANAGEMENT COMMENTS

September 26, 2016

Mr. Alvin Brown
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 2016 (Report No. A-ADF-16-00X-P)

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 President appoint in writing a senior-level Chief Information Security Officer in accordance with the Federal Information Security Modernization Act and the National Institute of Standards and Technology.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's President appoint in writing a senior-level Chief Information Security Officer in accordance with the Federal Information Security Modernization Act and the National Institute of Standards and Technology. Final action on this finding and recommendation will be completed by November 15, 2016.

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.

USADF Management Response: We accept the recommendation that the United 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 will include determining whether the security requirements and controls for the system are adequately documented and reflect the current information system environment. Final action on this finding and recommendation will be completed by June 30, 2017.

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.

USADF Management Response: We accept the recommendation 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 will include documenting assessment procedures to be used to determine security control effectiveness and testing the operating effectiveness of security controls. Final action on this finding and recommendation will be completed by June 30, 2017.

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.

USADF Management Response: We accept the recommendation 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. Final action on this finding and recommendation will be completed by July 15, 2017.

Recommendation No. 5: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to update all known security weaknesses and associated corrective plans quarterly as required by the foundation's policy and include them in the plan of action and milestones.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to update all known security weaknesses and associated corrective plans quarterly as required by the foundation's policy and include them in the plan of action and milestones. Final action on this finding and recommendation will be completed by December 15, 2016.

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.

USADF Management Response: We accept the recommendation 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. Final action on this finding and recommendation will be completed by May 30, 2017.

Recommendation No. 7: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to review and maintain an up-to-date information system inventory.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to review and maintain an up-to-date information system inventory. Final action on this finding and recommendation will be completed by December 1, 2016.

Recommendation No. 8: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to develop, document, and implement an enterprise architecture in accordance with National Institute of Standards and Technology standards.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to develop, document, and implement an enterprise architecture in accordance with National Institute of Standards and Technology Standard Publication 800-39. Final action on this finding and recommendation will be completed by May 15, 2017.

~~(SBU)~~ **Recommendation No. 9:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to perform [redacted].

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted]. Final action on this finding and recommendation will be completed by December 31, 2016.

~~(SBU)~~ **Recommendation No. 10:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] in accordance with the foundation's policy. This process should include ascertaining that [redacted] in accordance with policy.

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] in accordance with the foundation's policy. This process will include ascertaining that [redacted] in accordance with policy. Final action on this finding and recommendation will be completed by January 31, 2017.

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.

USADF Management Response: We accept the recommendation 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 will 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. Final action on this finding and recommendation will be completed by March 31, 2017.

~~(SBU)~~ **Recommendation No. 12:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] with the [redacted], including [redacted].

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] with the [redacted], including remediating any [redacted]. Final action on this finding and recommendation will be completed by February 15, 2017.

~~(SBU)~~ **Recommendation No. 13:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to remove users' administrator access to foundation workstations and prevent granting that access in the future. This process must include documenting the risk of such access and documenting the approval of any exceptions, along with adequate compensating controls.

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to remove users' administrator access to foundation workstations and prevent granting that access in the future. This process will include documenting the risk of such access and documenting the approval of any exceptions, along with adequate compensating. Final action on this finding and recommendation will be completed by February 28, 2017.

Recommendation No. 14: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to document, approve, and disseminate approved deviations from the United States Government Configuration Baseline settings.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to document, approve, and disseminate approved deviations from the United States Government Configuration Baseline settings. Final action on this finding and recommendation will be completed by March 15, 2017.

Recommendation No. 15: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to configure and regularly monitor password settings in accordance with the foundation's policy and encrypt passwords during authentication.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to configure and regularly monitor password settings in accordance with the foundation's policy and encrypt passwords during authentication. Final action on this finding and recommendation will be completed by March 15, 2017.

Recommendation No. 16: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to specify an organization-defined frequency for reviewing and updating the inventory of information system components.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's chief information security officer document and implement a process to specify an organization-defined frequency for reviewing and updating the inventory of information system components. Final action on this finding and recommendation will be completed by July 15, 2017.

Recommendation No. 17: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to maintain the inventory according to policy.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's chief information security officer document and implement a process to maintain the inventory according to policy. Final action on this finding and recommendation will be completed by July 15, 2017.

Recommendation No. 18: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to remove and decommission unused systems promptly.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to remove and decommission unused systems promptly. Final action on this finding and recommendation will be completed by July 31, 2017.

Recommendation No. 19: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to implement and enforce multifactor authentication for network access to privileged accounts.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to implement and enforce multifactor authentication for network access to privileged accounts. Final action on this finding and recommendation will be completed by August 31, 2017.

Recommendation No. 20: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to implement and enforce the use of personal identity verification credentials for access to the foundation's facilities, computers, and network.

USADF Management Response: We accept the recommendation that the United States Chief Information Security Officer document and implement a process to implement and enforce the use of personal identity verification credentials for access to the foundation's network and computers.

> **USADF Management Response:** Note: Access to the foundation's facility with use of personal identity verification (PIV) credentials is already enforced. Final action on this finding and recommendation will be completed by August 31, 2017.

~~(SBU)~~ **Recommendation No. 21:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted].

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's chief information security officer document and implement a process to [redacted]. Final action on this finding and recommendation will be completed by December 1, 2016.

Recommendation No. 22: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to review and analyze all required audit logs in accordance with the National Institute of Standards and Technology and the foundation's policy.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to review and analyze all required audit logs in accordance with the National Institute of Standards and Technology standards the foundation's policy. Final action on this finding and recommendation will be completed by April 15, 2017.

~~(SBU)~~**Recommendation No. 23:** We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] in accordance with the Office of Management and Budget and National Institute of Standards and Technology guidance given that the [redacted].

~~(SBU)~~ **USADF Management Response:** We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to [redacted] in accordance to the Office of Management and Budget (OMB Memorandum 07-16) and the National Institute of Standards and Technology guidance (NIST SP 800-21). Final action on this finding and recommendation will be completed by August 31, 2017.

~~(SBU)~~ **USADF Management Response:** Note: [redacted] are shared systems owned by [redacted] systems are shared systems owned by [redacted]. We will make efforts to obtain the [redacted] from the systems owners and [redacted].

Recommendation No. 24: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to maintain a current interconnection security agreement and memorandum of understanding between the foundation and the U.S. Department of Interior's Interior Business Center.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to maintain a current interconnection security agreement and memorandum of understanding between the foundation and the U.S. Department of Interior's Interior Business Center. Final action documenting will be completed by November 18, 2016.

Recommendation No. 25: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to provide annual security awareness training to overseas partners.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to provide annual security awareness training to overseas partners. Final action on this finding and recommendation will be completed by December May 31, 2017.

Recommendation No. 26: We recommend that the United States African Development Foundation's Chief Information Security Officer document and implement a process to provide annual role based training to all personnel with significant information security responsibilities.

USADF Management Response: We accept the recommendation that the United States African Development Foundation's Chief Information Security Officer document and implement a process to provide annual role based training to all personnel with significant information security responsibilities. Final action on this finding and recommendation will be completed by December 31, 2016.

/s/
C.D. Glin
President

cc: Mathieu Zahui, CFO
Solomon Chi, Supervisory Information Technology Specialist
Ellen Teel, Senior Auditor

SUMMARY OF RESULTS FOR EACH CONTROL REVIEWED

Control No.	Control Name	Is Control Effective?
General Support System		
AC-1	Access Control Policy and Procedures	Yes
AC-2	Account Management	Yes
AC-3	Access Enforcement	Yes
AC-17	Remote Access	Yes
AC-19	Access Control for Mobile Devices	Yes
AC-20	Use of External Information Systems	Yes
AT-1	Security Awareness and Training Policy and Procedures	Yes
AT-2	Security Awareness	No, See finding 8
AT-3	Security Training	No, See finding 8
AT-4	Security Training Records	Yes
AU-6	Audit Review, Analysis, and Reporting	No, See finding 5
CA-1	Security Assessment and Authorization Policies and Procedures	Yes
CA-2	Security Assessments	No, See finding 1, Security Authorization Process: Security Control Assessments
CA-5	Plan of Action and Milestones	No, See finding1, Plan of Action and Milestone Process
CA-6	Security Authorization	No, See finding1, Security Authorization Process
CA-7	Continuous Monitoring	No, See finding 5
CM-1	Configuration Management Policy and Procedures	Yes
CM-2	Baseline Configuration	No, See finding 3
CM-6	Configuration Settings	No, See finding 3
CM-7	Least Functionality	Yes
CM-8	Information System Component Inventory	No, See finding 3
CP-1	Contingency Planning Policy and Procedures	Yes
CP-2	Contingency Plan	Yes
CP-3	Contingency Training	No, See finding 9
CP-4	Contingency Plan Testing and Exercises	No, See finding 9
CP-9	Information System Backup	Yes
CP-10	Information System Recovery and Reconstitution	No, See finding 9

Control No.	Control Name	Is Control Effective?
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	No, See finding 4
IA-4	Identifier Management	No, See finding 4
IA-5	Authenticator Management	No, See finding 4
IA-6	Authenticator Feedback	Yes
IA-7	Cryptographic Module Authentication	Yes
IA-8	Identification and Authentication (Non-Organizational Users)	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-2	Incident Response Training	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-8	Incident Response Plan	Yes
PL-2	System Security Plan	No, See finding 1, Security Authorization Process: System Security Plans
PL-4	Rules of Behavior	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	No, See finding 6
RA-3	Risk Assessment	No, See finding 1, Security Authorization Process: Risk Assessments
RA-5	Vulnerability Scanning	No, See finding 2
SA-1	System and Services Acquisition Policy and Procedures	Yes
SA-5	Information System Documentation	Yes
SA-9	External Information System Services	Yes
SC-7	Boundary Protection	No, See finding 5
SI-2	Flaw Remediation	No, See finding 2
PM-1	Information Security Program Plan	Yes
PM-2	Senior Information Security Officer	No, See finding 1, Senior Information Security Officer
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	No, See finding 1, Plan of Action and Milestone Process
PM-5	Information System Inventory	No, See finding 1, Information System Inventory
PM-6	Information Security Measure of Performance	Yes

Control No.	Control Name	Is Control Effective?
PM-7	Enterprise Architecture	No, See finding 1, Enterprise Architecture
PM-8	Critical Infrastructure Plan	Yes
PM-9	Risk Management Strategy	No, See finding 1, Risk Management Strategy
PM-10	Security Authorization Process	No, See finding 1, Security Authorization Process
Program Support System		
AC-2	Account Management	Yes
AT-2	Security Awareness	No, See finding 8
AT-3	Security Training	Yes
CA-2	Security Assessments	No, See finding 1, Security Authorization Process: Security Control Assessments
CA-6	Security Authorization	No, See finding 1, Security Authorization Process
PL-2	System Security Plan	No, See finding 1, Security Authorization Process: System Security Plans
SA-9	External Information System Services	Yes
Payroll		
RA-2	Security Categorization	Yes
SA-9	External Information System Services	Yes
HR		
RA-2	Security Categorization	No, See finding 6
SA-9	External Information System Services	No, See finding 7
PRISM		
SA-9	External Information System Services	Yes
Oracle Financials		
RA-2	Security Categorization	Yes
SA-9	External Information System Services	Yes
Travel		
RA-2	Security Categorization	No, See finding 6
SA-9	External Information System Services	No, See finding 7

STATUS OF PRIOR YEAR FINDINGS

The following table provides the status of the FY 2015 FISMA Audit Recommendations.[20]

No.	FY 2015 Audit Recommendation	USADF Status	Auditor's Position on Status
1	We recommend that the United States African Development Foundation's Chief Financial Officer develop and fully implement a documented process to ensure that the agency's security assessment and authorization activities for systems transitioned to cloud service providers are compliant with NIST requirements. At a minimum, this should include a review of the security authorization package for the cloud service provider and a determination of risk to the agency documented in an authorization to operate memo based on a completed security controls assessment and updated system security plan, risk assessment and plan of action and milestones.	Closed	Disagree, See finding 1, Security Authorization Process, Recommendations 2, 3 and 4
2	We recommend that the United States African Development Foundation's Chief Financial Officer update the General Support System Security Plan to reflect NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.	Closed	Disagree, See finding 1, Security Authorization Process: System Security Plans, Recommendation 2
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.	Open	Agree, See finding 1, Security Authorization Process: System Security Plans, Recommendation 2

[20] *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).

No.	FY 2015 Audit Recommendation	USADF Status	Auditor's Position on Status
4	We recommend that the United States African Development Foundation's Chief Financial Officer develop and implement a documented process to ensure security assessment plans are documented for the General Support System that describe the scope of the assessment including security controls and control enhancements under assessment and assessment procedures to be used to determine security control effectiveness as required by NIST.	Open	Agree, See finding 1, Security Authorization Process: Security Control Assessments, Recommendation 3
5	We recommend that the United States African Development Foundation's Chief Financial Officer develop and fully implement a documented process to ensure that a security assessment is conducted annually for the General Support System as required by USADF policy.	Open	Agree, See finding 1, Security Authorization Process: Security Control Assessments, Recommendation 3
6	We recommend that the United States African Development Foundation's Chief Financial Officer develop and fully implement a documented process to enforce the required review of user accounts by system owners to ensure alignment with the individual's job function.	Closed	Agree
7	We recommend that the United States African Development Foundation's President appoint a Senior Agency Official for Privacy/Chief Privacy Officer who has the authority within the agency to consider information privacy policy issues at a national and agency-wide level.	Closed	Agree
8	We recommend that the United States African Development Foundation's President develop and fully implement a documented process to ensure that the Senior Agency Official for Privacy/Chief Privacy Officer meets privacy reporting requirements as stipulated by NIST and USADF policy.	Closed	Agree
9	We recommend that the United States African Development Foundation's President develop and fully implement a documented process to ensure that Privacy Impact Assessments are updated when a system change creates a new privacy risk and are reviewed and approved by the Senior Agency Official for Privacy/Chief Privacy Officer.	Closed	Agree
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.	Open	Disagree. Based on our testing, USADF has taken final corrective action on this recommendation.

No.	FY 2015 Audit Recommendation	USADF Status	Auditor's Position on Status
11	We recommend that the United States African Development Foundation's Chief Financial Officer develop and fully implement a documented process to ensure that the Contingency Plan for the General Support System and Program Support System is tested to ensure agency personnel are trained on how to respond in the event of a disruption of cloud-based services.	Open	Agree, See finding 9 Since management did not close this recommendation, an additional recommendation is not made at this time.
12	We recommend that the United States African Development Foundation's Chief Financial Officer develop and fully implement a documented process to ensure that contracts for service providers include requirements for security and privacy controls in compliance with USADF IT security policies, associated standards, and any applicable federal laws, directives, regulations, and guidance.	Closed	Agree

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
oig.usaid.gov
Audit Task No. AA100816