USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF UNITED STATES AFRICAN DEVELOPMENT FOUNDATION'S COMPLIANCE WITH PROVISIONS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

AUDIT REPORT NO. A-ADF-08-008-P
September 23, 2008

WASHINGTON, DC

USAID
FROM THE AMERICAN PEOPLE

Office of Inspector General

September 23, 2008

Lloyd Pierson, President
African Development Foundation
1400 I Street, NW
10th Floor
Washington, DC 20005

Subject: Audit of United States African Development Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2008 (Report No. A-ADF-08-008-P)

Dear Mr. Pierson:

This letter transmits our final report on the subject audit. In finalizing the report, we considered your comments on the draft report. Your comments are included in appendix II.

The report includes four recommendations to help the United States African Development Foundation improve its information security program. Based on our evaluation of your written comments, management decisions have been reached on all four recommendations. A determination of final actions must be made by the Foundation. Please notify us when final action is completed.

I appreciate the cooperation and courtesies extended to my staff during this audit.

Sincerely,

/s/

Joseph Farinella
Assistant Inspector General for Audit

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov

CONTENTS

Summary of Results 1

Background 2

Audit Objective 3

Audit Findings 4

USADF Information Security Policy Needs to Be Strengthened 4

USADF Needs to Develop an Inventory of All Information Systems 5

USADF Needs to Improve Initial Security Awareness and Training Program 6

USADF Needs to Implement Encryption on Laptop Computers 6

Status of Prior Year Recommendations 7

Evaluation of Management Comments 9

Appendix I – Scope and Methodology 10

Appendix II – Management Comments 12

SUMMARY OF RESULTS

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to establish an agencywide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source (see page 2). Since the United States African Development Foundation (USADF) is a Federal agency, it is required to comply with Federal information security requirements (see page 2). The objective of this audit was to determine if USADF's information security program met FISMA requirements (see page 3).

USADF's information security program generally complied with FISMA requirements. For example, in accordance with FISMA, USADF completed the certification and accreditation of its information systems, established an annual security awareness and training program, implemented adequate access controls to its information systems, complied with the Federal Desktop Core Configuration Requirements, and performed vulnerability scanning of its network on an ongoing basis (see page 4).

However, the audit found weaknesses in four areas. USADF did not (1) update its information security policy to reflect the current control environment and standards, (2) update its system inventory to include contractor systems, (3) implement an adequate security awareness program for new employees, and (4) implement encryption on all portable and mobile devices. Consequently, USADF's operations and assets may be at risk of misuse and disruption (see pages 4–7).

This report makes four recommendations to help USADF improve its information security program in the above four areas (see pages 4-7). In addition, the report provides an update of four audit recommendations from the fiscal year 2007 FISMA audit report[1] for which final action has not been completed. These recommendations addressed weaknesses in USADF's contingency plan testing, capital planning and investment control process, Privacy Act assessments, and information technology security performance measurements (see pages 7–8).

In response to the draft report, the USADF agreed with the audit findings and all four recommendations. USADF outlined its plans to address all four audit recommendations and provided target dates for when the final actions would be completed. Based on USADF's comments, management decisions have been reached on all four recommendations (page 9).

USADF's comments are included in their entirety in appendix II (see pages 12-13).

[1] Audit Report No.A-ADF-07-007-P, *Audit of African Development Foundation's Compliance with Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2007*, dated September 20, 2007.

BACKGROUND

In 1980, the United States Congress established the United States African Development Foundation (USADF) (also known as the African Development Foundation) as an independent public corporation with a mandate to promote participation by Africans in the economic and social development of their countries. For more than 20 years, USADF has helped grassroots groups and individuals in Africa help themselves by providing the resources they need to advance their own efforts to promote economic and social development. Because USADF is a Federal agency, it is required to comply with Federal information security requirements.

The Federal Information Security Management Act of 2002 (FISMA) was enacted into law under Title III of Public Law 107-347 on December 17, 2002. Key requirements of FISMA include the following:

1. The establishment of an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
2. An annual independent evaluation of the agency's information security programs and practices; and
3. An assessment of compliance with the requirements of the Act.

FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management is integrated with agency strategic and operation 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.

At the time of the audit, USADF operated two information systems[2]: (1) Wide Area Network and (2) Program Support System. USADF also used three systems operated by the Department of Interior's National Business Center. This audit focused on the systems operated by USADF.

[2] Federal Information Processing Standards 199 defines three levels of potential impact that a system and its information can have on an organization if a security breach should occur. USADF categorized its two information systems as "Low", which is defined as a limited adverse effect on individuals, organizational operations and assets.

AUDIT OBJECTIVE

A key requirement of the Federal Information Security Management Act of 2002 is an annual independent evaluation of USADF's information security program. The objective of this audit was to answer the following question:

> Did the United States African Development Foundation's information system security program meet the requirements of the Federal Information Security Management Act of 2002?

Appendix I contains a discussion of the audit's scope and methodology.

AUDIT FINDINGS

The United States African Development Foundation's (USADF) information security program generally complied with the requirements of the Federal Information Security Management Act of 2002 (FISMA) for fiscal year (FY) 2008. USADF had implemented 47 of 50 tested security controls that are required by FISMA. During FY 2008, USADF devoted significant time and resources to developing security enhancements to improve its information systems and as a result, generally complied with FISMA requirements such as the following:

- Completing the certification and accreditation of its information systems.
- Conducting annual security awareness training for its current employees.
- Implementing adequate access controls for its information systems.
- Complying with the Federal Desktop Core Configuration Requirements.
- Scanning its network routinely to identify and fix security vulnerabilities.

However, the audit found weaknesses in four areas of USADF's information systems security program. USADF did not (1) update its information security policy to reflect current control environment and standards, (2) update its system inventory to include contractor systems, (3) implement an adequate initial security awareness program for new employees, and (4) implement encryption on its portable laptop computers. In addition, USADF had not addressed four outstanding audit recommendations that identify weaknesses in its contingency plan testing, capital planning and investment control process, implementing Privacy Act assessments, and developing information technology security performance measurements. Consequently, USADF's operations and assets may be at risk of misuse and disruption. These issues are discussed on pages 4–7.

USADF Information Security Policy Needs to Be Strengthened

National Institute of Standards and Technology NIST Special Publication 800-53, Revision 1, Control PL-1, *Security Planning Policy and Procedures*, states that agencies should develop, disseminate, and periodically review/update (1) a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance and (2) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

USADF's Manual Section (MS) 462, *IT Security Program Policy and Minimum Implementation Standards,* documents USADF's information technology policies and procedures. MS 462 defines USADF's information technology security program requirements and its implementation for all USADF operating units and employees, both

Federal and contractor. Although USADF has documented its information technology policies and procedures in MS 462, it has not been updated since 2004 to reflect the security controls contained in NIST Special Publication 800-53, Revision 1. Consequently, it reflects controls from NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* that has since been superseded by NIST Special Publication 800-53, Revision 1. USADF had not updated the policy manual because the USADF considered its System Security Plans (SSP) to be the source for detailed policies and procedures, and system-specific control implementations. However, if policies and procedures that comprise USADF's information technology program are outdated, there is a risk that they may not adequately address the current security control needs of USADF's systems and information technology security control environment.

> *Recommendation No. 1: We recommend that the United States African Development Foundation update its policies and procedures document, Manual Section 462,* IT Security Program Policy and Minimum Implementation Standards*, to address relevant security controls identified by the National Institute of Standards and Technology Special Publication 800-53, Revision 1,* Recommended Security Controls for Federal Information Systems*.*

USADF Needs to Develop an Inventory of All Information Systems

According to FISMA, "The head of each agency shall develop and maintain an inventory of major information systems operated by or under the control of such agency." FISMA also states that the system inventory shall be updated annually and include "an identification of the interfaces between each such system and all other systems or networks." In addition, NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, Configuration Management - 8, *Information System Component Inventory,* states that organizations should develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.

Contrary to FISMA and NIST requirements, USADF did not include all the information systems that support the operations and assets of USADF on its system inventory. USADF's internal systems (Wide Area Network and Program Support System) were included in the system inventory; however, the following contractor systems were not included: Federal Personnel Payroll System (FFPS), Oracle Federal Financial System (OFF), and CW Government Travel's System. In addition, the inventory had not been formally approved by USADF management.

The CIO stated that USADF did not maintain an approved inventory of systems, which included external contractor systems, such as Federal Personnel Payroll System, Oracle Federal Financial System, and CW Government Travel's System. However, without a completed and approved inventory of all systems USADF has not identified all the information systems that need to be monitored for compliance with FISMA.

Recommendation No. 2: We recommend that the United States African Development Foundation update and formally approve its inventory of systems to include all information systems that support the operations and assets of the Foundation.

USADF Needs to Improve Initial Security Awareness and Training Program

The National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 1, *AT-2 Security Awareness*, states, "The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and *at least annually* thereafter." NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, also includes guidance for security awareness training program and identifies 27 recommended topics for security awareness training. USADF however did not include all security awareness topics in its training program.

USADF provided initial security awareness training to new personnel by providing them with USADF's Computer System Access Agreement Form. However, the form covered only 6 of the 27 security awareness topics from NIST Special Publication 800-50. USADF personnel stated that additional topics may be covered; however, documentation of new personnel receiving additional training topics was not maintained. Consequently, the failure to establish adequate initial security awareness documentation and guidance for training new users increases the risk associated with misuse of information technology and possible infrastructure exploitation caused by uninformed personnel.

Recommendation No. 3: We recommend that the United States African Development Foundation implement and document for new personnel security awareness training that includes the 27 topics, as appropriate, that are included in the National Institute of Standards and Technology Special Publication *Special Publication 800-50, Building an Information Technology Security Awareness and Training Program.*

USADF Needs to Implement Encryption on Laptop Computers

Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Agency Information,* states that agencies are to "encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

USADF had encrypted its portable BlackBerry devices, but had not implemented encryption on its laptop computers. Information security personnel were aware of the

requirement to have encryption on portable and mobile devices and were investigating the rollout of laptop encryption on the USADF's three laptop computers. However, without encryption on portable and mobile devices, USADF's information is at a greater risk of being compromised.

> *Recommendation No.4: We recommend that the United States African Development Foundation implement encryption on all its laptop computers.*

Status of Prior Year Recommendations

Although USADF is making progress implementing an information systems security program to comply with the requirements set out in FISMA, it had not completed final action on the four following FISMA-related recommendations made during the FY 2007 FISMA audit[3]. The status of each of the recommendations is discussed below.

Fiscal Year 2007 FISMA Audit Recommendations:

> *Recommendation No. 3: We recommend that the United States African Development Foundation test its contingency plan and train its personnel with contingency plan responsibilities as required by the National Institute of Standards and Technology's Special Publication 800-34.*

FY 2008 Update: USADF updated its contingency plan during FY 2008; however, testing of the plan had not occurred. USADF is investigating the possibility of a reciprocal agreement with another Federal agency for the use of a shared hot site for disaster recovery. Consequently, final action on this recommendation had not occurred.

> *Recommendation No. 4: We recommend that the United States African Development Foundation implement an information technology capital planning and investment controls process to comply with the National Institute of Standards and Technology's Special Publication 800-65.*

FY 2008 Update: USADF had not made progress on this recommendation due to changes in senior management and USADF's other priorities. Consequently, final action on this recommendation had not occurred.

> *Recommendation No. 5: We recommend that the African Development Foundation develop and implement procedures to perform privacy impact assessments as required.*

FY 2008 Update: USADF implemented a policy manual defining the USADF's privacy program to include roles and responsibilities within the program, and policy directives and required procedures that establish the program's function and purpose. The policy manual included procedures for conducting Privacy Act assessments; however, USADF had not completed Privacy Act assessments for its information systems. Consequently, final action on this recommendation had not occurred.

[3] Audit Report No. A-ADF-07-007-P, *Audit of African Development Foundation's Compliance with Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2007*, dated September 20, 2007.

Recommendation No. 6: We recommend that the United States African Development develop and implement procedures to (a) measure information technology security performance, and (b) link security performance to the agency's strategic goals and objectives to comply with the National Institute of Standards and Technology's draft Special Publication 800-80.

FY 2008 Update: USADF had not made progress on this recommendation due to changes in senior management and the USADF's other priorities. Consequently, final action on this recommendation had not occurred.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the United States African Development Foundation (USADF) agreed with the audit findings and the four recommendations made in the report. USADF outlined its plans to address all four audit recommendations and described planned actions to address the recommendations. USADF's comments are included in their entirety in appendix II.

For Recommendations 1, 2, 3, and 4, USADF described and outlined its plans to address the audit recommendations and provided target dates for when the final actions would be completed. Based on USADF's comments and the establishment of target dates, management decisions have been reached for each of these recommendations.

SCOPE AND METHODOLOGY

Scope

The audit was designed to answer the following question: Did the United States African Development Foundation's information system security program meet the requirements of the Federal Information Security Management Act (FISMA) of 2002? The audit fieldwork was performed at the USADF headquarters in Washington, DC, from June 23 to August 15, 2008.

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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 1, *Recommended Security Controls for Federal Information Systems,* to assess USADF's performance and compliance with FISMA in the following areas:

- Configuration management.
- Risk assessments.
- Logical access controls.
- Physical and environmental protection.
- Certification and accreditation process.
- Security awareness and training.

In addition, a vulnerability assessment of USADF's computer servers and demilitarized zone[4] was performed using Nessus vulnerability scanning software. We did not scan USADF's desktop computers. A copy of our vulnerability scanning results was provided to USADF's management.

The audit also included a followup on prior year audit recommendations to determine if USADF had made progress on implementing the recommended improvements concerning its information security program.

During the audit period, USADF operated two information systems: (1) the Wide Area Network and (2) Program Support Systems, which consist of the Grant Management Database System and the USADF Website. In addition, USADF used three systems operated by the Department of Interior's National Business Center (NBC). USADF relied on its memorandums of understanding with NBC and independent audits for security

[4] In computer security, a **demilitarized zone** (DMZ) is a physical or logical subnetwork that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add a layer of security to an organization's Local Area Network; an external attacker has access only to equipment in the DMZ, rather than the whole of the network.

assurances for the three systems operated by NBC. The focus of this audit was on the systems operated by USADF.

Methodology

To determine if USADF's information security program met FISMA requirements, we interviewed USADF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, USADF's (1) information technology (IT) contingency plan, (2) plan of action and milestones, (3) certification and accreditation package for major systems, and (4) IT security program policy. Where appropriate, we compared documents, such as the contingency plan and security plans, to requirements stipulated by the National Institute of Standards and Technology's special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

We also reviewed the status of the FY 2007 FISMA audit recommendations.[5]

[5] Audit Report No. A-ADF-07-007-P, *Audit of African Development Foundation's Compliance with Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2007,* dated September 20, 2007.

MANAGEMENT COMMENTS

September 15, 2008

Mr. Joseph Farinella
Assistant Inspector General for Audit
USAID, Officer of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523

Subject: African Development Foundation Response to the Draft Audit Report On ADF's Compliance with FISMA.

Dear Mr. Farinella:

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 2002. We have reviewed your report and have the following comments in response to your recommendations.

1. **We recommend that the United States African Development Foundation update its policies and procedures document, Manual Section 462, IT Security Program Policy and Minimum Implementation Standards, to address relevant security controls identified by the National Institute of Standards and Technology Special Publication 800-53, Revision 1, Recommended Security Controls for Federal Information Systems.**

   We accept the finding with the following comment. The security plans for both ADF systems were revised to reflect the security controls identified NIST's Special Publication 800-53 (Revision 1) and approved and placed in our Manual Section last year. Our Manual Section 462, IT Security Program Policy and Minimum Implementations Standards which provides guidance on the general conditions in which our systems operate also needs to be revised to reflect this more complete set of security controls. The revision of our Manual Section 462 is scheduled for completion in the first quarter of FY 2009.

2. **We recommend that the United States African Development Foundation update and formally approve its inventory of systems to include all information systems that support the operations and assets of the Foundation.**

We accept the finding with the following comment. The system inventory provided showed only the two ADF owned systems. A new system inventory will be put in place before the end of FY 2008.

3. **We recommend that the United States African Development Foundation implement and document for new personnel security awareness training that includes the 27 topics, as appropriate, that are included in the National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program.**

   We accept the finding with the following comment. ADF will expand its security awareness training for new personnel to include all 27 topics found in the National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program. The training will be in the form of a concise written document that the new employee will be asked to review and then sign as an acceptance and understanding of Federal security issues as they enter on duty. We will keep the signature page as a record of the training. We will complete work for this recommendation before the end of the first quarter of FY 2009

4. **We recommend that the United States African Development Foundation implement encryption on all its laptop computers.**

   We accept the finding with the following comment. At the time of the audit, USADF had begun but not completed the process of reviewing specifications for encryption products. In its selection, ADF will ensure that the product will meet or exceed requirements found in FIPS 140-2 and National Institute of Standards and Technology Special Publication 800-20 Guideline for Implementing Cryptography in the Federal Government. This procurement will be completed before the end of the first quarter of FY 2009.

Again, we appreciate the cooperation and support of your staff in working with us during the audit process, and look forward to a new year with continuing improvements to our information security.

Sincerely,

/s/

Lloyd O. Pierson
President

cc: Doris Mason Martin, GC
Larry Bevan, CIO
[redacted]

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Ave, NW
Washington, DC 20523
Tel: (202) 712-1150
Fax: (202) 216-3047
www.usaid.gov/oig