USAID
FROM THE AMERICAN PEOPLE

OFFICE OF INSPECTOR GENERAL

AUDIT OF AFRICAN DEVELOPMENT FOUNDATION'S COMPLIANCE WITH PROVISIONS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2007

AUDIT REPORT NO. A-ADF-07-007-P

September 20, 2007

WASHINGTON, DC

Office of Inspector General

September 20, 2007

Rodney MacAlister, President
African Development Foundation
1400 I Street, NW
10th Floor
Washington, DC 20005

Subject: Audit of African Development Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2007 (Report No. A-ADF-07-007-P)

Dear President MacAlister:

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

This report contains seven recommendations to help the African Development Foundation strengthen its information security program. Based on our evaluation of your written comments, management decisions have been reached on all seven recommendations. A determination of final actions must be made by the Foundation. Please notify us of the Foundation's actions.

I appreciate the cooperation and courtesy extended to each of the members of my staff during the audit.

Sincerely,

[*Alvin Brown for*] /s/

Joseph Farinella
Assistant Inspector General for Audit

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

Some of the information contained in this report may be "Sensitive But Unclassified."

CONTENTS

SUMMARY OF RESULTS

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement an agencywide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. The objective of this audit was to determine if the African Development Foundation's (ADF) information security program met FISMA requirements (page 3).

This audit, which was performed by the Office of Inspector General's Information Technology and Special Audits Division, meets the FISMA requirement for an annual evaluation of ADF's information security program (page 2).

Although ADF complied with some FISMA requirements, it needed to strengthen several areas to improve its information security program. For example, in accordance with FISMA, ADF updated its inventory of major information systems, conducted periodic risk assessments of its three information systems, and established baseline security configuration checklists for several systems. However, it did not meet six key FISMA requirements. ADF did not (1) comply with Federal guidance when developing security plans, (2) include required procedures in its contingency plan, (3) implement a capital planning and investment control process, (4) develop procedures for privacy impact assessments, (5) develop information technology security performance measurements, or (6) develop certain configuration management procedures. Consequently, ADF's operations and assets may be at risk of misuse and disruption (pages 4 to 11).

This report makes seven recommendations to assist ADF in strengthening its information security program (pages 7 to 11). In response to our draft report, ADF agreed with the audit findings and all seven recommendations. ADF outlined its plans to address the audit recommendations and provided target dates for when the final actions would be completed. Based on ADF's comments, management decisions have been reached on all seven recommendations (page 12). ADF's comments are included in their entirety in Appendix II to this report (page 15).

BACKGROUND

In 1980, the United States Congress established the African Development Foundation (ADF) 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, ADF 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 ADF is a Federal agency, it is required to comply with Federal information security requirements.

ADF has 37 employees. ADF's information technology (IT) department consists of the chief management officer (CMO) and a contractor who acts as the network administrator for ADF's information systems. The CMO also served as the chief information officer (CIO), information system security officer (ISSO), and the system owner for ADF's local area network (LAN) and Web site. (In July 2007, the CMO changed job responsibilities to become the full-time CIO and no longer serves as the CMO.) As network administrator, the contractor is responsible for providing qualified and responsive management and technical professional computer support services and assistance to ADF staff.

The Federal Information Security Management Act of 2002 (FISMA), which was enacted into law as Title III of the E-Government Act of 2002 (P.L. 107-347, December 17, 2002) states,

> *Each agency shall develop, document, and implement 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.…*

FISMA provides the framework for securing the Federal Government's information technology. All agencies must implement FISMA requirements and report annually to the Office of Management and Budget (OMB), congressional committees, and the Government Accountability Office (GAO) on the effectiveness of their security systems. The reports must include independent evaluations by the agency inspector general. In addition, FISMA 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, ADF operated three information systems[1]: (1) General LAN, (2) Grants Management Database, and (3) Web site. ADF also used two systems operated by the Department of Interior's National Business Center (NBC). This audit focused on the three systems operated by ADF. The fiscal year 2007 budget for ADF's information management support was approximately $1.3 million.

[1] ADF categorized its three information systems as "moderate," as prescribed by Federal Information Processing Standards 199.

AUDIT OBJECTIVE

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

> Did the 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 African Development Foundation's (ADF) information security program complied with some requirements of the Federal Information Security Management Act of 2002 (FISMA); however, ADF needed to strengthen several areas to improve its security program.

During fiscal year 2007, ADF devoted significant time and resources to developing security enhancements to improve its information systems. As a result of its efforts, ADF generally complied with the following FISMA requirements:

- Updating its inventory of major information systems
- Conducting periodic risk assessments for its three information systems
- Establishing baseline security configuration checklists for desktops, servers, and routers
- Scanning its network routinely to identify and fix security vulnerabilities

However, the audit found weaknesses in six areas of ADF's information systems security program. ADF did not (1) comply with Federal guidance when developing security plans, (2) include required procedures in its contingency plan, (3) implement a capital planning and investment control process, (4) develop procedures for privacy impact assessments, (5) develop information technology security performance measurements, or (6) develop certain configuration management procedures. These issues are discussed on pages 5 to 11.

ADF's Information Systems Security Program Needed to Strengthen Several FISMA Requirements to Improve Security

Summary: The African Development Foundation (ADF) complied with some requirements of the Federal Information Security Management Act of 2002 (FISMA); however, it needed to strengthen the following six key areas to improve its information security program.

- Comply with Federal guidance when developing security plans.
- Include required procedures in its contingency plan.
- Implement a capital planning and investment control process.
- Develop procedures to perform privacy impact assessments.
- Develop procedures to measure information technology security performance measurements.
- Develop certain configuration management procedures.

Among the reasons for ADF's noncompliance in these areas were time constraints and other priorities faced by the agency. Consequently, ADF's operations and assets may be at risk of being compromised because of the information systems security weaknesses.

According to FISMA, "Each agency shall develop, document, and implement 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…." These requirements include, among others, the following:

- Developing security plans to comply with Federal guidance
- Preparing a contingency plan
- Implementing a capital planning and investment control process
- Performing privacy impact assessments
- Developing information technology security performance measurements
- Adhering to and developing configuration management procedures

ADF did not meet these six FISMA requirements for its information program. Each of these issues is discussed below.

1. **Security plans need to comply with Federal guidance –** The National Institute of Standards and Technology (NIST) Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides an overview of the security requirements of an entity's information systems and describes the

minimum security control procedures that need to be in place or planned for the system to meet those requirements. For example, it states that the security plan should document and clearly describe all minimum security requirements in this standard by applying controls selected in accordance with NIST Special Publication 800-53, *Guide for Assessing the Security Controls in Federal Information Systems*. NIST Special Publication 800-18 also states that security plans should be reviewed and updated at least annually.

To its credit, ADF developed three security plans in September 2004—plans that were acceptable in several respects. The security plans, however, did not fully comply with NIST Special Publication 800-18. Specifically, the three security plans did not document and describe the minimum security control procedures that need to be in place or planned or provide reasons why various controls were not implemented. For example, the plans did not include eight selected control procedures from NIST Special Publication 800-53. Table 1 below identifies those eight control procedures:

Table 1: Summary of the control procedures not documented in ADF's three security plans.

Control Numbers	Selected NIST Special Publication 800-53 Control Procedures
PL-3	Agency procedures should update the security plan to address system changes or problems identified during implementation or security control assessments.
AC-2	Agency procedures describe how to manage information accounts, including establishing, activating, reviewing, and removing accounts.
AC-17	Agency procedures should document, monitor, and control all methods of remote access.
AC-19	Agency establishes usage restrictions and implementation guidance for portable and mobile devices; monitors and controls the use of portable and mobile devices; and authorizes the use of portable and mobile devices.
AU-3	Agency information systems capture sufficient information in audit records to establish what events occurred, the sources of events, and the outcomes of the events.
AU-6	Agency procedures describe how to regularly review audit records for indication of inappropriate or unusual activity, investigate unusual activity, and report findings to appropriate officials.
CM-7	Agency procedures describe how to review the information system to provide only essential capabilities and restrict the use of the following functions, ports, protocols, and services.
MP-1.2	Agency media-handling policies are adequate to address the purpose, scope, responsibilities, management commitment, coordination among entities, and compliance.

In addition, the security plans had not been reviewed and updated annually—all three plans were developed and last updated in September 2004. For instance, in January 2007, ADF's network expanded to include its regional office in Ghana; however, the agency's General Local Area Network security plan was not updated to describe the minimum security controls in place (or planned) for the network in Ghana.

Without documenting and describing controls in ADF's security plans, the security controls may be inadequate or improperly implemented. Inadequate or improper security controls may not provide sufficient protection for sensitive or critical resources.

ADF's information technology (IT) team is very small, and the responsibility for describing minimum security controls in place or planned for each of the three systems is shared with ADF's information system security officer (ISSO) and a contractor who acts as the network administrator for ADF's information systems. The ISSO and the network administrator also function in other capacities within ADF and had not identified the minimum security controls or updated the security plans because of other priorities faced by the agency. Because the ISSO no longer serves as chief management officer as of July 2007 and may have more time to devote to his responsibilities as ISSO, we are not making a recommendation that addresses the ISSO's divided responsibilities and other priorities.

At the time of the audit, ADF was in the process of replacing its three existing information systems with two new information systems: the Wide Area Network System and the Program Support Systems. The audit did not include the two new systems because they were not deployed until after the audit fieldwork was complete. Since ADF had not developed and finalized the security plans for its new systems, and its existing security plans were no longer suitable, we are making the following recommendation to ensure that the security plans for the new information systems meet NIST requirements:

> *Recommendation 1: We recommend that the African Development Foundation develop and implement the following two security plans: (a) Wide Area Network System and (b) Program Support Systems, to fully comply with the National Institute of Standards and Technology's Special Publication 800-18.*

2. **Required procedures not included in contingency plan (repeat finding)**[2] **–** NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, provides specific instructions for restoring critical systems, including instructions for arranging alternative processing facilities in case the usual facilities are damaged or cannot be accessed because of unexpected events such as a temporary power failure or a major disaster. It is important that these plans be tested to determine whether the plans will function as intended in an emergency. Such tests determine whether the alternative work site will function as intended and whether critical computer data and programs to be recovered from off-site storage

[2] Audit Report No.A-ADF-06-001-P, "Audit of the African Development Foundation's Compliance with the Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2006," dated September 28, 2006.

will be accessible and current. Moreover, these tests should train personnel who have contingency plan responsibilities to carry out their roles and responsibilities during a disaster.

Contrary to the contingency planning guidance contained in NIST Special Publication 800-34, ADF did not include the following specific procedures in its contingency plan:

- Damage assessment
- Recovery procedures
- Media protection
- Shut-down and restart processes or procedures
- Alternate storage site of back-up tapes
- Alternate work site
- Detailed hardware and software recovery process

In addition, ADF did not test the plan, and ADF personnel had not been trained to implement their contingency responsibilities.

The ISSO and the administrator had not tested the contingency plan because of time constraints. Without a comprehensive contingency plan, ADF may not be able to recover quickly and effectively from a service disruption, disaster, or other emergency.

As previously reported, the OIG identified that ADF did not include specific procedures in its contingency plan. The report did not make a recommendation because ADF's Plan of Action and Milestones, dated June 15, 2006, indicated a plan to update the contingency plan by August 2006. Because ADF did not update its contingency plan, we are making the following recommendations:

Recommendation 2: We recommend that the African Development Foundation revise its contingency plan to fully comply with the National Institute of Standards and Technology's Special Publication 800-34.

Recommendation 3: We recommend that the 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.

3. **Information technology capital planning and investment control process needed –** NIST Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, helps Federal agencies integrate IT security into their capital planning and investment controls (CPIC) processes. This guidance introduces common criteria against which agencies can prioritize security activities, and ensures that needed corrective actions are incorporated into the capital planning process to provide maximum security and financial benefit to the agency. As part of the capital planning process, an Exhibit 300 document must be submitted to OMB for all major IT acquisitions and ongoing major IT investments for reporting and budgeting requirements.

ADF, however, did not implement an IT capital planning and investment controls process and did not prepare an Exhibit 300 document for its major IT acquisitions. At the time of the audit, ADF operated three major IT systems. The CIO stated that although he was aware of the requirement for a CPIC process and understood its importance, ADF had not yet developed a CPIC process because it had not developed procedures for planning, budgeting, and managing its IT capital assets. ADF developed guidance on life-cycle processes which states, as part of its system acquisition process, that an Exhibit 300 document should be prepared. The guidance, however, was not adequate because it did not ensure that IT acquisitions were selected, monitored, and evaluated effectively for implementation. Without an IT CPIC process, ADF cannot fully ensure that it will have effective investment management, maximum IT security, and the financial benefits provided by these components. Therefore, we are making the following recommendation:

Recommendation 4: We recommend that the 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.

4. **Procedures for privacy impact assessments needed –** OMB defines a privacy impact assessment (PIA) as an analysis of how information is handled to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

   In addition, FISMA requires agencies to complete PIAs before (1) developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form about an individual or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons, excluding agencies, instrumentalities, or employees of the Federal Government.

   Although PIAs are required, ADF did not conduct any PIAs for its planned information systems. ADF has a policy that addresses safeguarding private information;[3] however, the agency did not develop procedures to ensure that PIAs would be conducted when required. Completed PIAs would benefit the agency because the CIO stated that ADF's IT systems do contain sensitive information, such as individual names, addresses, and bank account numbers. Failing to conduct PIAs increases the risk of harm from unauthorized release of sensitive information. Further, ADF could not ensure that sensitive information is handled in a manner that maximizes privacy. Therefore, we are making the following recommendation:

[3] ADF's policy for safeguarding private information was addressed in 22 CFR pt. 1507, "Rules Safeguarding Personal Information."

Recommendation 5: We recommend that the African Development Foundation develop and implement procedures to perform privacy impact assessments as required.

5. **Security program needs performance measurements –** NIST draft Special Publication 800-80, *Guide for Developing Performance Metrics for Information Security*, provides instructions to develop and implement effective and efficient metrics. Information security metrics provide a means for monitoring and reporting an agency's implementation of security controls. They also help assess the effectiveness of these controls in protecting agency information resources in support of the agency's mission. Further, the processes and methodologies described in the guide demonstrate how to link information security performance to the agency's strategic goals and objectives.

   ADF did not develop IT security metrics and track IT security performance. Specifically, no metrics were used to demonstrate progress in implementing individual IT security controls. Some examples of metrics that could be used include (1) the percentage of employees who have signed an acknowledgement that they have read and understood information system security policies and procedures; (2) the percentage of system users who have received basic awareness training; and (3) the frequency with which the organization analyzes audit records for violations. Other metrics are available to quantify outcomes by applying security controls described in NIST Special Publication 800-53.

   ADF did not develop IT security performance metrics because it did not have agency-specific procedures to (1) develop and implement effective and efficient metrics and (2) link information security performance to the agency's strategic goals and objectives. Without performance measures, agency resources were allocated to IT security with no metrics to demonstrate how the information security program improved or supported the organization's missions. Therefore, we are making the following recommendation:

   Recommendation 6: We recommend that the African Development Foundation 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.

6. **Certain configuration management procedures need to be developed and followed –** NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products*, was issued to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. Configuration management is the process by which the configuration of a system and its components are identified and documented, and changes are controlled and tracked. System configuration includes a security configuration checklist, which is a document that contains instructions or procedures for configuring an IT product to a baseline level of security. The goal of configuration management is to facilitate detection of any changes to hardware and software within an information system.

To its credit, ADF developed baseline security configuration checklists for desktops, servers, and routers. However, some configuration management areas still contained security weaknesses. (1) Some procedural controls for moderate-risk systems were not developed, and (2) some procedures were developed but not fully followed.

Developing procedures: ADF's configuration management procedures did not incorporate applicable control procedures recommended in NIST Special Publication 800-53. For example, ADF did not have the following procedural controls in place: (1) establishment of mandatory configuration settings, (2) configuration settings for essential capabilities, and (3) restriction of access privileges for making changes. The ISSO and the network administrator also functioned in other capacities throughout the agency and had not included security controls in the procedures because the agency faced other priorities at the time.

Following procedures: ADF developed some configuration management procedures for documenting and authorizing changes; however, the network administrator for ADF's information systems did not follow prescribed procedures or use required forms to document and authorize configuration changes. For example, e-mail correspondence was used instead of prescribed forms. The network administrator did not realize the importance of completing all required forms before changing the configuration. Not using all the required forms increases the likelihood of unauthorized changes to the system.

By incorporating minimum configuration management controls described in NIST Special Publication 800-53, ADF could increase the probability of faster problem resolution, greater levels of security, faster resolution of service, and a more effective and efficient change management. Therefore, we are making the following recommendation:

> *Recommendation 7: We recommend that the African Development Foundation (a) develop configuration management procedures to include all appropriate recommended National Institute of Standards and Technology Special Publication 800-53 controls, and (b) comply with the Foundation's configuration management procedures.*

EVALUATION OF MANAGEMENT COMMENTS

In response to our draft report, the African Development Foundation (ADF) agreed with the audit findings and described planned actions to address the recommendations. The Foundation's comments are included in their entirety in Appendix II.

For Recommendations 1, 2, 3, 4, 5, 6, and 7, ADF outlined its plans to address the audit recommendations and provided target dates for when final action would be completed. Based on ADF's comments and the establishment of target dates, management decisions have been reached for each of these recommendations.

SCOPE AND METHODOLOGY

Scope

The Office of Inspector General, Information Technology and Special Audits Division, conducted this audit in accordance with U.S. generally accepted government auditing standards. The audit was designed to answer the following question: Did the African Development Foundation's information system security program meet the requirements of the Federal Information Security Management Act of 2002 (FISMA)?

The audit covered the period from October 1, 2006, through August 21, 2007. The audit fieldwork was performed at the African Development Foundation's (ADF) headquarters in Washington, D.C., from June 4, 2007, to August 21, 2007, and covered FISMA-related areas including the following:

- Establishing information security performance measures
- Establishing procedures for detecting, reporting, and responding to security incidents
- Establishing configuration management policies and procedures
- Establishing procedures for a capital planning and investment control process for information technology systems
- Establishing processes to manage remedial action used to address deficiencies
- Assessing risk periodically
- Testing and evaluating the effectiveness of its security policies
- Establishing and documenting continuity of operations plans
- Certifying and accrediting its information systems

ADF operated three information systems: (1) General Local Area Network (LAN), (2) Grants Management Database, and (3) Web site. The audit included the above systems and a review of draft documents associated with two systems planned by ADF that will replace the existing three information systems. The planned systems were to be deployed after our audit fieldwork. In addition, ADF used two systems operated by the Department of Interior's National Business Center (NBC). ADF relied on its memoranda of understanding with NBC and independent audits for security assurances for the two systems operated by NBC. The focus of this audit was on the three systems operated by ADF. ADF's fiscal year 2006 FISMA audit report was also reviewed.

Methodology

To determine if ADF's information security program met FISMA requirements, we conducted interviews with ADF 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, ADF's (1) information technology (IT) contingency plan; (2) quarterly plan of action and milestones; (3) inventory of 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 (NIST) special publications. We selected eight control procedures from NIST Special Publication 800-53 to test whether selected control procedures were described in the three security plans. We also reviewed the status of the fiscal year 2006 FISMA audit recommendation.[4] To evaluate the security of ADF's major systems, we performed vulnerability scans to detect system vulnerabilities using Nmap and Nessus.[5] We did not determine materiality thresholds for the audit objective.

[4] Audit Report No.A-ADF-06-001-P, "Audit of the African Development Foundation's Compliance with the Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2006," dated September 28, 2006.

[5] Nmap is a commonly used port scanner for identifying active hosts and associated services. Nessus is a vulnerability scanner and audit tool used to test known vulnerabilities.

MANAGEMENT COMMENTS

September 5, 2007

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 the time and effort your staff has spent in working with the Foundation in improving the management of our information security and in coming into 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 African Development Foundation develop and implement the following two security plans (1) Wide Area Network System, and (2) Program Support Systems to fully comply with the National Institute of Standards and Technology Special Publication 800-18.**

   We accept the finding with the following comment. As relayed during the audit, USADF is in the process of finalizing system security plans for both of the new systems mentioned in your recommendation. While both plan revisions were initiated to anticipate changes in our system structure and the deployment of USADF's Wide Area Network, we also are taking this opportunity to incorporate appropriate security control procedures from NIST SP 800-53 and requirements from NIST SP 800-18, which were not a part of the original plans. With planned certification and accreditation of the two new systems this fiscal year, we plan to have final, approved security plans in place before September 30, 2007.

2. **We recommend that the African Development Foundation revise its contingency plan to fully comply with the National Institute of Standards and Technology Special Publication 800-34.**

   We accept the finding with the following comment. USADF has started the process of developing and performing initial tests on a Continuity of Operations Plan (COOP) of which our contingency plans are a part. This initial work on the Foundation's COOP pointed out the needs, also identified in this recommendation, to better describe processes and procedures and then train responsible Foundation personnel. We agree that the contingency plan has to be revised to include specific procedures outlined in NIST SP 800-34; be more specific in identifying and assigning plan responsibilities; be effectively disseminated to all responsible parties through training: and, be tested. Our goal is to revise the contingency plan prior to the end of this fiscal year.

3. **We recommend that the 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 Special Publication 800-34.**

   We accept the finding with the following comment. We recognize that before it can be a functional part of our overall COOP, the contingency plan first has to be made a part of our regular and established practices at the Foundation. After the plan is revised, (see recommendation Number 2) we plan to train responsible parties and complete testing within the first quarter of FY 2008.

4. **We recommend that the African Development Foundation implement and follow an information technology capital planning and investment control process to comply with the National Institute of Standards and Technology Special Publication 800-34.**

   We accept the finding with the following comment. The audit correctly points out that USADF has never developed a Capital Planning and Investment Control process following the guidance in OMB Circular A-11 for Exhibit 300. We intend to contact the Foundation's OMB examiner to discuss the exact process. Pending their recommendation, we will make plans to submit Exhibit 300 for this year's OMB Submission or plan for next. In either case, we will be reviewing NIST SP 800-65 to ensure our compliance with that guidance.

5. **We recommend that the African Development Foundation develop and implement procedures to perform privacy act assessments as required.**

We accept the finding with the following comment. As the audit identified, USADF does have a policy that addresses safeguarding private information, however, we have not yet developed procedures to perform privacy impact assessments. While our existing policy does cause us to consider privacy issues when developing and implementing our systems, USADF recognizes that conducting structured privacy impact assessments would better help us to mitigate potential privacy risks. To respond to this recommendation, USADF will revise its privacy policies to require privacy impact assessments and develop procedures for carrying them out by the second quarter in FY 2008.

6. **We recommend that the African Development Foundation develop and implement procedures to (1) develop and implement effective and efficient metrics, and (2) link information security performance to the agency's strategic goals and objectives to comply with the National Institute of Standards and Technology Special Publication 800-80.**

   We accept the finding with the following comment. USADF will take steps to develop and implement metrics that will link information security performance to the Foundation's strategic goals and objectives by the second quarter of FY 2008.

7. **We recommend that the African Development Foundation: (1) update configuration management procedures to include all appropriate recommendations in NIST Special Publication 800-53, and (2) comply with its configuration management procedures.**

   We accept the finding with the following comment. USADF will review its current configuration management procedures and make changes to more fully employ the controls found in NIST SP 800-53 and update our checklists to conform to criteria in NIST SP 800-70. These revisions will be completed by the end of the second quarter of FY 2008.

At the time of the writing of this response, new security plans are nearing final approval and will be in place to satisfy our overall goal to certify and accredit our two new systems ADF-001 Wide Area Network and ADF-002 Program Support Systems. 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/

Rodney J. MacAlister
President

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