OFFICE OF INSPECTOR GENERAL

AUDIT OF THE INTER-AMERICAN FOUNDATION'S COMPLIANCE WITH PROVISIONS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2010

AUDIT REPORT NO. A-IAF-10-003-P
SEPTEMBER 22, 2010

WASHINGTON, D.C.

Office of Inspector General

September 22, 2010

Ms. Linda Borst Kolko, Interim President
Inter-American Foundation
901 North Stuart Street, 10th Floor
Arlington, VA 22203

Subject: Audit of the Inter-American Foundation's Compliance With Provisions of the Federal Information Security Management Act for Fiscal Year 2010 (Report No. A-IAF-10-003-P)

Dear Ms. Kolko:

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

The report includes one recommendation to help the Inter-American Foundation improve its information security program. Based on our evaluation of your written comments, a management decision has been reached on the recommendation. A determination of final action must be made by the Foundation. Please notify us when final action has been completed.

I want to express my sincere appreciation for the cooperation and courtesies extended to my staff during the audit.

Sincerely,

/s/

Joseph Farinella
Assistant Inspector General for Audit

CONTENTS

Summary of Results..1

Audit Findings..3

The Foundation Had Not Performed a
Tabletop Exercise for Contingency Planning..3

Foundation Policy on Access Control
Did Not Include Publicly Accessible Content 4

Evaluation of Management Comments..5

Appendix I – Scope and Methodology...6

Appendix II – Management Comments..8

SUMMARY OF RESULTS

The Federal Information Security Management Act of 2002[1] requires 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 Inter-American Foundation (the Foundation) 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 capability is established, and (3) information security management is integrated with the agency's strategic and operation planning processes. All agencies must also report annually on the effectiveness of their information security program. In addition, the act made the standards issued by the National Institute of Standards and Technology (NIST) mandatory for federal agencies.

A key requirement of the act is an annual independent evaluation of agencies' information security programs and practices. The U.S. Agency for International Development's Office of Inspector General (OIG) conducted this audit to determine whether the Foundation implemented selected security controls[2] for selected information systems in support of the Federal Information Security Management Act of 2002.

At the time of the audit, the Foundation operated two information systems: (1) the Enterprise Network and (2) the Grant Evaluation Management System. The Enterprise Network provides the infrastructure that supports mission-critical and mission-important applications as well as administrative and minor applications for the Foundation. The Grant Evaluation Management System tracks all grant activity for the Foundation.

The audit found that the Foundation had generally implemented selected security controls for its information security program. For example, the Foundation:

- Integrated security training into its new employee orientation and annual refresher training for employees.

- Documented comprehensive and up-to-date policies and procedures for responding to computer incidents, intrusions, and emergencies.

- Established a baseline configuration management process.

Although the Foundation had implemented many security controls over its information systems, the audit identified two weaknesses in the Foundation's information security program.

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002), and codified at 44 U.S.C. 3541-3549 (2006).

[2] The table in Appendix I lists selected controls.

Specifically, the audit found that:

- The Foundation had not performed a tabletop exercise for contingency planning as required by Foundation policy. A tabletop exercise is an element of contingency planning. It involves personnel meeting in a classroom or other group setting to discuss their roles during an emergency and their responses to a particular emergency. Tabletop exercises do not involve deploying equipment or other resources (page 3).

- Foundation policy on access control did not include publicly accessible content as recommended in NIST Special Publication 800-53, Revision 3 (page 4).

After our exit conference, Foundation officials provided OIG staff an updated access control policy that incorporates publicly accessible content. As a result, the report makes only one recommendation to the Foundation's Chief Information Officer to conduct a tabletop exercise for contingency planning as required by the Foundation's continuity of operations policy (page 3).

Appendix I details the audit's scope and methodology. Appendix II contains the Foundation's comments in their entirety. OIG has reviewed the information provided by the Foundation in its response to the draft report and determined that a management decision has been reached on the recommendation.

AUDIT FINDINGS

The Foundation Had Not Performed a Tabletop Exercise for Contingency Planning

National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, CP-4, "Contingency Plan Testing and Exercises," states that, "The organization tests and/or exercises the contingency plan for the information system to determine the plan's effectiveness and the organization's readiness to execute the plan."

The Foundation's *c*ontinuity of operations policy states, "The Foundation shall develop and maintain detailed business, communications, and IT recovery plans, and the associated recovery capability in the event that normal operations are disrupted. All personnel involved with planning efforts shall be identified and trained in executing the plan and recovery capability." The policy also states that the Foundation shall review and update the plan annually; according to the Foundation's information system security officer (ISSO), the annual requirement includes conducting a tabletop exercise.

A tabletop exercise is an element of contingency planning. It involves personnel meeting in a classroom or other group setting to discuss their roles during an emergency and their responses to a particular emergency. Tabletop exercises do not involve deploying equipment or other resources.

However, contrary to the Foundation's continuity of operations policy, the Foundation did not conduct a tabletop exercise as a part of its annual contingency planning to ensure that key Foundation personnel understood and discussed their roles in executing the recovery plan for an emergency.

The Foundation's ISSO stated that the tabletop exercise was not conducted because the focus for contingency planning was on testing the systems and conducting phone tree exercises.

By not conducting tabletop exercises, the Foundation runs the risk of not being able to recover as quickly and effectively as possible following an emergency. To reduce that risk, this audit makes the following recommendation.

> ***Recommendation****.* *We recommend that the Inter-American Foundation's Chief Information Officer schedule and conduct a tabletop exercise with key personnel in support of the Inter-American Foundation's continuity of operations policy.*

Foundation Policy on Access Control Did Not Include Publicly Accessible Content

NIST Special Publication 800-53, Revision 3, AC-22, “Publicly Accessible Content,” states that: “The organization (a) designates individuals authorized to post information onto an organizational information system that is publicly accessible; and (b) trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.”

The Foundation’s information security manual does not fully incorporate all relevant controls identified by NIST Special Publication 800-53. Specifically, access control policy and procedures for publicly accessible content are missing from the Foundation’s manual.

Although the Foundation has a process for authorizing and training individuals responsible for Web posting of publicly accessible content, the Foundation has not documented this process in its information security manual. By not documenting authorization and training processes in its access control policy, the Foundation runs the risk that personally identifiable information may inadvertently be released to the public.

The ISSO stated that the control was not incorporated into the access control policy because of an oversight. After our exit conference, the Foundation’s ISSO submitted to OIG an updated access control policy that incorporates publicly accessible content as required by NIST Special Publication 800-53. As a result, we are not making a recommendation that addresses the publicly accessible content requirement.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Inter-American Foundation (the Foundation) agreed with the audit finding and the recommendation. The Foundation indicated that it is working with contract information technology security specialists from the Bureau of the Public Debt to plan and implement a tabletop exercise with key Foundation personnel no later than March 31, 2011. The Foundation's comments are included in their entirety in Appendix II.

The Office of Inspector General has reviewed the Foundation's response and determined that a management decision has been reached on the recommendation.

SCOPE AND METHODOLOGY

Scope

This audit was designed and performed by USAID's Office of Inspector General (OIG), Information Technology Division to answer the following question: Did the Inter-American Foundation implement selected security controls for selected information systems in support of the Federal Information Security Management Act of 2002?

The audit was conducted at the Foundation's headquarters in Arlington, Virginia, from May 10 through July 16, 2010. We conducted this performance 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 in accordance with our audit objective. We believe that the evidence obtained provides that reasonable basis.

At the time of the audit, the Foundation had two information systems: (1) the Enterprise Network and (2) the Grant Evaluation Management System. The Department of the Treasury's Bureau of Public Debt's Information Technology Group provides network administration and information systems security for both systems. The Foundation also used two systems operated by outside entities—a payroll system operated by the Department of Interior's National Business Center and a financial management system operated by the Department of Treasury's Bureau of Public Debt. This audit assessed selected controls on the two systems operated by the Foundation.

Methodology

OIG staff conducted interviews with key personnel and obtained and reviewed control policies, procedures, and system documentation. We gained an understanding of system operations and identified significant computer operations through discussions with Foundation officials including the information system security officer.

Following the framework for minimum security controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, dated August 2009,[3] we selected certain controls (shown in the table on the next page) from NIST security control families[4] and reviewed the selected controls over the Foundation's Enterprise Network and the Grant Evaluation Management System.

[3] NIST publications take effect 1 year from their publication date. For this audit, we followed Revision 3 of NIST 800-53, which took effect before this report's publication.

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

Selected Security Controls

NIST Control Family	Control Name
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-7	Unsuccessful Logon Attempts
AC-22	Publicly Accessible Content
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AT-4	Security Training Records
CA-1	Security Assessment and Authorization Policies and Procedures
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CA-6	Security Authorization
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-4	Contingency Plan Testing and Exercises
IR-1	Risk Assessment Policy and Procedures
IR-2	Incident Response Training
IR-4	Incident Handling
IR-6	Incident Reporting
PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PM-2	Senior Information Security Officer
PM-4	Plan of Action and Milestones Process
RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
RA-3	Risk Assessment

MANAGEMENT COMMENTS

Inter-American Foundation

An Independent Agency of the U.S. Government

September 17, 2010

Joseph Farinella
Assistant Inspector General for Audit
U.S. Agency for International Development
1300 Pennsylvania Avenue, N.W.
Washington, DC 20523

Subject: Comments on Audit Report of IAF Compliance with Provisions of the Federal Information Security Management Act (FISMA) for Fiscal Year 2010

Dear Mr. Farinella:

Thank you very much for sharing the draft report prepared by the USAID Office of the Inspector General on the FY 2010 annual audit of the Inter-American Foundation's (IAF) information security program. The IAF has reviewed the report and concurs with the accuracy of your assessment that IAF generally implemented selected security controls in compliance with FISMA requirements.

We also are in agreement with the recommendation cited in the audit report for IAF to conduct a tabletop exercise as one of the annual planning and testing elements our continuity of operations policy. While the IAF successfully conducted systems tests and phone tree exercises with employees during FY 2010, we did not include a tabletop exercise with staff to review roles and responsibilities for executing our recovery plan for an emergency event. We are working with contract IT security specialists from the Bureau of the Public Debt to plan and implement such a tabletop exercise with key IAF personnel no later than March 31, 2011, in keeping with the agency's continuity of operations policy.

Once again, I would like to take this opportunity to recognize the high level of professionalism of the USAID OIG audit team that conducted the FY 2010 audit of IAF's security posture. The auditor who performed the site review demonstrated an impressive knowledge of IT security and related federal guidelines, and was thoroughly briefed by the OIG team on the state of IAF's security, all of which contributed to the efficiency of the audit process. The auditor scheduled informational interviews with a cross-section of staff without disruption to productivity and offered many helpful suggestions to further strengthen our IT security program. We value the advice and work of your office, and look forward to our continued collaboration.

Sincerely,

/s/

Linda B. Kolko
Interim President

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
www.usaid.gov/oig