OFFICE OF INSPECTOR GENERAL

AUDIT OF THE INTER-AMERICAN FOUNDATION'S FISCAL YEAR 2011 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

AUDIT REPORT NO. A-IAF-12-001-P
OCTOBER 21, 2011

WASHINGTON, D.C.

Office of Inspector General

October 21, 2011

Mr. Robert N. Kaplan, President
Inter-American Foundation
901 North Stuart Street, 10th Floor
Arlington, VA 22203

Subject: Audit of the Inter-American Foundation's Fiscal Year 2011Compliance With the Federal Information Security Management Act of 2002 (Report No. A-IAF-12-001-P)

Dear Mr. Kaplan:

The U.S. Agency for International Development (USAID) Office of Inspector General (OIG), Information Technology Division, is transmitting the final audit report prepared by Clifton Gunderson LLP on the subject audit. In finalizing the report, we considered your comments on the draft report and included them in their entirety as Appendix II. The report does not contain any recommendations, and there is no additional action required by your office to address the report's finding.

The Federal Information Security Management Act of 2002 requires federal 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 act also requires agencies to have an annual evaluation of their information security program and practices.

In support of the act's requirements, Clifton Gunderson LLP was engaged to conduct an audit to determine whether the Inter-American Foundation implemented selected security controls for selected information systems. Appendix I contains a list of the selected security controls and information systems.

The audit concluded that the Inter-American Foundation (IAF) had implemented selected security controls for selected information systems in support of the act. For example, IAF maintained an effective security-awareness training program for its employees, implemented access controls over the organization's Enterprise Network and Grant Evaluation Management System, and established an effective continuous monitoring program. However, Clifton Gunderson LLP noted that IAF was not encrypting its data on backup tapes to be transferred off-site. IAF personnel took immediate corrective action during the audit to encrypt the organization's data on backup tapes. Because corrective action occurred before the completion of the audit, the report makes no recommendation on this finding.

We have evaluated your written comments and noted your agreement with our assessment that IAF implemented selected security controls in support of the Federal Information Security Management Act of 2002.

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

Sincerely,

/*s*/

Tim Cox
Assistant Inspector General for Audit

cc: Vice-President of Operations
Director of Information and Management Systems

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

COUNT ON INSIGHT®

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Audit of the Inter-American Foundation's Compliance with the Federal Information Security Management Act of 2002

Fiscal Year 2011

Final Report

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

CONTENTS

Summary of Results.....1

Audit Findings.....3

Data Was Not Encrypted
On Backup Tapes 3

Evaluation of Management Comments.....4

Appendix I – Scope and Methodology 5

Appendix II – Management Comments 8

SUMMARY OF RESULTS

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

The audit was performed in support of the FISMA requirement for an annual evaluation of IAF's information security program. The objective of this audit was to determine whether the Inter-American Foundation implemented selected[2] security controls for selected information systems in support of the Federal Information Security Management Act of 2002.

At the time of the audit, IAF operated two information systems: the Enterprise Network and 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 IAF. The Grant Evaluation Management System tracks all grant activity for IAF.

The audit concluded that IAF had generally implemented selected security controls for its information security program. For example, IAF:

- Maintained an adequate and effective security awareness and training program for its employees including new employee orientation and annual refresher training.

- Implemented adequate access controls over the Enterprise Network and the Grant Evaluation Management System.

- Established an effective continuous monitoring program.

Although IAF had implemented many security controls over its information systems, the audit identified one weakness in the IAF's information security program. Specifically:

- IAF was not encrypting data on backup tapes to be transferred offsite.

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C. 3541-3549.

[2] See Appendix I for a list of controls selected.

However, IAF personnel took immediate corrective action to encrypt the data stored on its backup tapes. As a result, the report does not make any recommendations. The details of the finding are discussed in the following section.

Appendix I contains details of the audit's scope and methodology. Appendix II contains IAF's comments in their entirety, and our evaluation of management comments is included in the report on page 4.

AUDIT FINDINGS

Data Was Not Encrypted On Backup Tapes

The Inter-American Foundation was not encrypting its data on backup tapes prior to their being sent to the offsite facility.

National Institute of Standards and Technology Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, security control MP-4, "Media Storage," states the following regarding Information System Backups:

> The organization:
>
> a. Physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] using [Assignment: organization-defined security measures];
> b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
>
> Control Enhancement:
> (1) The organization employs cryptographic mechanisms to protect information in storage.

IAF's Chief Information Security Officer (CISO) indicated that IAF had ceased encrypting backups due to the extended time requirements and insufficient tape storage capacity for full-encrypted backups to complete. Although the CISO stated that the IAF stores tape backup media in locked cases during transfer; this does not satisfy National Institute of Standards and Technology media storage encryption requirements.

By not encrypting data on its backup tapes, IAF is at an increased risk that lost or stolen tapes may disclose sensitive data to unauthorized personnel. After noting this, IAF personnel took immediate corrective action and re-enabled the encryption of data on backup tapes. Moreover, IAF personnel indicated that they are seeking to procure a new backup tape library with encryption-enabled drives and larger tape storage capacity to replace the existing unit, which they plan to implement by September 2011. As a result of IAF's actions, the audit is not making a recommendation at this time.

EVALUATION OF MANAGEMENT COMMENTS

The report does not contain any recommendations. In response to the draft report, the Inter-American Foundation (IAF) concurs with the accuracy of our assessment that IAF implemented selected security controls in support of the Federal Information Security Management Act. IAF's comments are included in their entirety in Appendix II.

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with generally accepted government auditing standards.[3] 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 a reasonable basis for our findings and conclusions based on our audit objective.

This audit was designed by USAID's Office of the Inspector General (OIG), Information Technology Audit Division, and performed by Clifton Gunderson, LLP to answer the following question: Did the Inter-American Foundation implement selected[4] security controls for selected information systems in support of the Federal Information Security Management Act of 2002?

At the time of the audit, the Inter-American Foundation (IAF) had two information systems: the Enterprise Network and the Grant Evaluation Management System. IAF also used two systems operated by outside entities—a payroll system operated by the Department of Interior's National Business Center (NBC) and a financial management system operated by the Department of Treasury's Bureau of Public Debt (BPD). This audit assessed selected controls on the two systems operated by IAF, evaluated 3rd party independent reports (e.g., SAS 70, SSAE 16, IG reports), and the most recent service level agreements of IAF's external service providers – NBC and BPD.

The audit was conducted at IAF's headquarters in Arlington, Virginia, from July 18 through September 6, 2011.

Methodology

Following the framework for minimum security controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, dated August 2009, certain controls (shown in the table on the next page) were selected from NIST security control families.[5] We reviewed the selected controls over IAF's Enterprise Network and the Grant Evaluation Management System.

To accomplish our audit objective, we interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA. We also reviewed documentation related to IAF's information security program, such as security policies and procedures, system security plans, and disaster recovery plans. In addition, we tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix I). Furthermore, we reviewed the 3rd party independent reports and the most recent service level agreements of the IAF's external service providers (NBC and BPD). We also

[3] Government Auditing Standards, July 2007 Revision (GAO-07-731G).
[4] See Appendix I for a list of controls selected.
[5] Security controls are organized into families according to their security function—for example, access controls.

reviewed the status of FISMA audit report[6] recommendations for FY 2010. We determined that corrective actions have been taken on all prior audit recommendations.

SELECTED SECURITY CONTROLS

NIST Control Number	Control Name	Enterprise Network	GEMS
AC-1	Access Control Policy & Procedures	X	
AC-2	Account Management		X
AC-5	Separation of Duties		X
AC-7	Unsuccessful Login Attempts		X
AC-8	System Use Notification	X	
AC-17	Remote Access	X	
AC-19	Access Control for Mobile Devices	X	
AT-1	Security Awareness and Training Policy and Procedures	X	
AT-2	Security Awareness	X	
AU-1	Audit and Accountability Policy and Procedures	X	
AU-9	Protection of Audit Information	X	
CA-1	Security Assessment and Authorization Policies and Procedures	X	
CA-7	Continuous Monitoring	X	
CP-1	Contingency Planning Policy and Procedures	X	
CP-2	Contingency Plan		X
CP-3	Contingency Training	X	
CP-9	Information System Backup	X	X
IA-1	Identification and Authentication Policy and Procedures	X	
IA-4	Identifier Management	X	
IA-7	Cryptographic Module Authentication	X	
MA-1	System Maintenance Policy and Procedures	X	
MA-2	Controlled Maintenance	X	
MP-1	Media Protection Policy and Procedures	X	
MP-5	Media Transport	X	
PE-1	Physical and Environmental Protection Policy and Procedures	X	
PE-6	Monitoring Physical Access	X	
PE-7	Visitor Control	X	
PE-10	Emergency Shutoff	X	
PE-12	Emergency Lighting	X	
PE-13	Fire Protection	X	
PE-14	Temperature and Humidity Controls	X	
PE-15	Water Damage Protection	X	
PE-16	Delivery and Removal	X	

[6] 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).

PE-17	Alternate Work Site	X	
PL-1	Security Planning Policy and Procedures	X	
PL-4	Rules of Behavior	X	
PS-1	Personnel Security Policy and Procedures	X	
PS-4	Personnel Termination	X	
PS-5	Personnel Transfer	X	
SC-1	System and Communications Protection Policy and Procedures	X	
SC-13	Use of Cryptography	X	
SC-28	Protection of Information at Rest	X	
SI-1	System and Information Integrity Policy and Procedures	X	
SI-5	Security Alerts, Advisories, and Directives	X	
SI-11	Error Handling	X	

Inter-American Foundation

An Independent Agency of the U.S. Government

October 11, 2011

Tim Cox
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 2011

Dear Mr. Cox:

Thank you very much for sharing the draft report prepared by the USAID Office of the Inspector General on the FY 2011 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 implemented selected security controls for selected information systems in support of the Federal Information Security Management Act.

I would like to take this opportunity to express our appreciation for the fine work and high level of professionalism of the USAID AIG team that conducted the FY 2011 audit of the IAF information assurance program. We were very favorably impressed with their methodology and well-defined work plan, as well as their extensive technical knowledge of IT security, all of which contributed to the efficiency and thoroughness of the review. We are continually seeking ways in which to further strengthen our security posture, and look forward to our continued collaboration.

Sincerely,

/s/

Robert N. Kaplan
President & CEO

901 N. Stuart Street • Arlington, VA 22203 • Phone: 703-306-4301 • Fax: 703-306-4369

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