OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018

AUDIT REPORT A-IAF-19-003-C
NOVEMBER 2, 2018

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

Office of Inspector General, U.S. Agency for International Development

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: November 2, 2018

TO: Inter-American Foundation, President and CEO, Paloma Adams-Allen

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

SUBJECT: IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (A-IAF-19-003-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2018. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown and Company CPAs and Management Consultants PLLC (Brown) to conduct the audit. The contract required Brown to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Brown's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on IAF's compliance with FISMA. Brown is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Brown did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether IAF implemented selected security controls for certain information systems in support of FISMA. To answer the audit objective, Brown evaluated IAF's implementation of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Specifically, Brown reviewed selected controls for IAF's sole internal information system and for two of nine external systems. The firm also performed a vulnerability assessment of IAF's internal system and an evaluation of IAF's process for identifying and mitigating technical vulnerabilities. Fieldwork was performed at IAF's headquarters in Washington, DC, from April 17 through September 6, 2018.

The audit firm concluded that IAF generally complied with FISMA by implementing 63 of 72 security controls reviewed for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems. Among the controls IAF effectively implemented were the following:

- Change management policy and procedures.
- Procedures for security awareness and training.
- Information system continuous monitoring.
- Account management procedures for bringing on new employees and ensuring terminated employees' access is removed timely.

However, IAF did not implement nine controls related to risk management, governance, continuity of operations, network vulnerabilities, and multifactor authentication.

To address the weaknesses identified in the report, we recommend that IAF's chief information officer:

Recommendation 1. Develop and implement an enterprise risk management policy that fully defines the Foundation's risk management policies, procedures, and strategy, including the organization's processes and methodologies for (1) categorizing risk, (2) developing a risk profile, (3) assessing risk and risk appetite/tolerance levels and responding to risk, and (4) monitoring risk.

Recommendation 2. Create a change control board or related oversight body, composed of knowledgeable individuals from across functional departments that reviews, approves, and manages changes to configuration items, and ensure that the oversight body develops a configuration management plan that documents roles and responsibilities and configuration management processes, including (1) identifying and managing configuration items at the appropriate point in an organization's software development; (2) performing configuration monitoring; and (3) applying configuration management requirements to contracted systems. The plan should also ensure that the originator and approver of changes are not the same person.

Recommendation 3. Test and exercise the Foundation's continuity of operations plan and document the specific test and exercise activities conducted, along with their results.

Recommendation 4. Remediate configuration-related vulnerabilities in the network identified by the Office of Inspector General, as appropriate, and document the results or document acceptance of the risks of those vulnerabilities.

In finalizing the report, the audit firm evaluated IAF's responses to the recommendations. We reviewed that evaluation and consider all four recommendations resolved but open pending completion of planned activities. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance extended to our staff and Brown's employees during the engagement.

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, document, and implement an information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA also requires agencies to have an annual assessment of their information systems.

We contracted with the independent certified public accounting firm Brown and Company CPAs and Management Consultants PLLC to conduct an audit of IAF's compliance with FISMA during fiscal year 2018. The audit firm concluded that IAF generally complied with FISMA requirements by implementing 63 of 72 selected security controls for selected information systems. However, IAF did not implement nine controls that safeguard the confidentiality, integrity, and availability of its information and information systems. To address the weaknesses identified, OIG made four recommendations. The audit firm evaluated IAF's responses to the recommendations. We reviewed that evaluation and consider all four recommendations resolved but open pending completion of planned activities.