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 Inter-American Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018

Final Report

October 22, 2018

Prepared by

Brown & Company CPAs and Management Consultants, PLLC
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Mr. Mark S. Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Mr. Norman:

Enclosed is our report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The Inter-American Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018*. The U.S. Agency for International Development Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs and Management Consultants, PLLC to conduct the audit in support of the FISMA requirement for an annual evaluation of IAF's information security program.

The objective of this performance audit was to determine whether IAF implemented selected security controls for certain information systems in support of FISMA. 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

For this audit, we reviewed selected controls from IAF's three information systems. The audit also included a vulnerability assessment of IAF's general support system and an evaluation of IAF's process for identifying and mitigating information systems vulnerabilities. Audit fieldwork was performed at the Inter-American Foundation's headquarters in Washington, D.C., from April 17, 2018 through September 6, 2018.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit concluded that IAF generally complied with FISMA requirements by implementing many selected security controls for selected information systems. Although IAF generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

Consequently, the audit identified areas in IAF's information security program that needed to be improved. We are making four recommendations to assist IAF in strengthening its information security program. In addition, findings related to three recommendations from prior years were not yet fully implemented, and therefore, new recommendations were not made.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of IAF and the opportunity to serve you. We will be pleased to discuss any questions you may have.

Brown & Company CPAs and Management Consultants, PLLC
October 22, 2018
Largo, Maryland

TABLE OF CONTENTS

Summary of Results

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems[2], including those provided or managed by another agency, contractor, or other source. Because the Inter-American Foundation (IAF or Foundation) is a federal agency, it is required to comply with federal information security requirements.

FISMA 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 to the Office of Management and Budget (OMB) and to 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 (NIST) are mandatory for Federal agencies.

The U.S. Agency for International Development (USAID) Office of Inspector General engaged us, Brown & Company CPAs and Management Consultants, PLLC to conduct an audit in support of the FISMA requirement for an annual evaluation of IAF's information security program. The objective of this performance audit was to determine whether IAF implemented selected security controls for certain information systems in support of FISMA.

Our audit was performed 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this audit we reviewed selected controls from one IAF-managed system and two applications managed by external contractors.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002.
[2] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Results

We concluded that IAF generally complied with FISMA by implementing 63 of 72[3] security controls reviewed for selected information systems. For example, IAF did the following:

- Implemented effective change management policy and procedures.
- Implemented effective security awareness and training procedures.
- Implemented an effective Information Security Continuous Monitoring automated process.
- Implemented effective processing procedures for bringing on new employees and ensuring terminated employee access was removed timely.

Although IAF generally had policies for its information security program, its implementation of those policies for 9 of 72 security controls reviewed was not fully effective to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in IAF's information security program that needed to be improved. Specifically, IAF needs to:

- Improve the documentation of its risk management policy, procedures, and strategy.
- Establish a change governance structure, such as Change Control Board (CCB), to identify, review, approve, and document system configuration setting changes.
- Test its Continuity of Operations (COOP) Plan to ensure the availability and effectiveness of the plan,
- Mitigate network vulnerabilities, and
- Implement prior years' recommendations.

As a result, IAF's operations and assets may be at risk of unauthorized access, misuse and disruption. This report makes four recommendations to assist IAF in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to 3 of 6 prior year recommendations had not yet been fully implemented, and therefore, new recommendations were not made. Detailed findings appear in the following section.

[3] See Appendix IV for the number of selected controls tested.

Audit Findings

IAF Needs to Improve Its Risk Management Policy, Procedures, and Strategy

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security and risk management policy procedure, and program. A comprehensive risk assessment program starts with clear policy and procedure that delineates roles and responsibilities to serve as a starting point for developing or modifying an agency's security policies and plans. A risk assessment that is performed based on established policy and procedures should consider threats and vulnerabilities that are specific to an agency, its system, and applications, and consider risks to data confidentiality, integrity, and availability.

NIST Special Publication (SP) 800-53, Revision 4 (Rev.4), *Security and Privacy Controls for Federal Information Systems and Organizations*, security control RA-1, Risk Assessment Policy and Procedures, states the following:

> The organization:
>
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
>
> 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
>
> b. Reviews and updates the current:
>
> 1. Risk assessment policy; and
> 2. Risk assessment procedures.

In addition, security control PM-9, Risk Management Strategy, requires a federal agency to:

a. Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
b. Implement the risk management strategy consistently across the organization; and
c. Review and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, requires the development of organizational specific, as opposed to a generic, risk management policy with the development of a comprehensive governance structure and organization-wide risk management strategy, at entity and system level.

NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, provides guidance around managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and

individuals.

The Chief Financial Officers Council's *Playbook: Enterprise Risk Management [ERM] for the U.S. Federal Government* provides high-level key concepts for consideration when establishing a comprehensive and effective ERM program and aligns with guidelines presented via OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

The Foundation has not fully documented a risk management strategy addressing how it intends to assess, respond to, and monitor information security risk at the organizational level as required by NIST SP 800-39. Such a strategy would make explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions.

IAF's *Information Security Manual*, Revision 4, dated July 2011, defines high-level policies and procedures to support its agency-wide information security risk management program. In March 2017, IAF issued *Information System Security Program Standard Operating Procedures*. The purpose of these operating procedures was:

> *To serve as a foundational document for The Inter-American Foundation's Information System Security Program by establishing guidelines and procedures for ensuring an adequate level of information security for all unclassified information to include sensitive data and Personally Identifiable Information (PII) processed, transmitted, stored or disseminated on the Agency's information systems.*

Neither the Manual nor the Operating Procedures fully define the Agency's risk management policies, procedures, and strategy that include:

- the organization's processes and methodologies for categorizing risk,
- developing a risk profile,
- assessing risk, risk appetite/tolerance levels, responding to risk, and
- Monitoring risk.

IAF's security control "Risk Management Strategy" (PM-9), states "*IAF develops a comprehensive strategy to manage risk to IAF operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems*." IAF is in the process of implementing the security control, but had not yet fully implemented it. By not fully documenting its risk management strategy and risk management policies, procedures, IAF is at risk of not being able to rank and quantify risks that would allow the Foundation to efficiently and effectively direct resources to its most prevalent challenges.

> **Recommendation 1:** We recommend that the Inter-American Foundation's Chief Information Officer develop and implement an enterprise risk management policy that fully defines the Foundation's risk management policies, procedures, and strategy, including (a) the organization's processes and methodologies for categorizing risk; (b) developing a risk profile; (c) assessing risk and risk appetite/tolerance levels and responding to risk; and (d) monitoring risk.

IAF Needs to Establish a Change Governance Structure, Such as a Change Control Board

NIST SP 800-53, Rev. 4, security control CM-1, Configuration Management Policy and Procedures, states:

> The organization:
>
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
>
> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
>
> b. Reviews and updates the current:
>
> 1. Configuration management policy [Assignment: organization-defined frequency]; and
> 2. Configuration management procedures [Assignment: organization-defined frequency]; and

In addition, security control CM-3, Configuration Change Control, states:

> The organization:
>
> a. Determines the types of changes to the information system that are configuration-controlled;
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
> c. Documents configuration change decisions associated with the information system;
> d. Implements approved configuration-controlled changes to the information system;
> e. Retains records of configuration-controlled change
> f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
> g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

IAF's System Security Plan (SSP) for an internal system was updated in October 2017 and states:

> **Configuration Change Control (CM-3)**
> IAF implements change control using a Change Control Board and change request forms. A separate request is required for each change. IAF uses maintenance changes, emergency changes, and major changes. Each request is reviewed by the System Security Officer and if considered secure, is approved. The IAF tests, validates, and documents changes before implementing the change to the system. The change requests and the decisions about them are maintained by the System Security Officer.

We noted that:

- IAF has not formalized a change governance structure, such as a CCB, composed of knowledgeable individuals from cross-functional departments, that reviews and approves all software changes and changes to baselined configuration items; to ensure that all proposed changes receive appropriate technical analysis, review, and to ensure that changes are documented for tracking and auditing purposes.
- IAF has not fully developed a standard CM plan to ensure that changes are made within an application system in a consistent manner, and the appropriate stakeholders are informed of the state of the product, changes to it and the cost and schedule impact of these changes.

IAF's management stated that there is an informal process that delegates the Chief Information Officer and the Chief Information Security Officer to review and approve configuration changes. This, however, doesn't constitute a formal CCB or change control committee composed of additional knowledgeable individuals from cross functional departments or offices to provide oversight for configuration change control activities, as recommended by NIST SP 800-53, Rev. 4.

> **Recommendation 2:** We recommend that the Inter-American Foundation's Chief Information Officer:
>
> a. Create a Change Control Board or related oversight body, composed of knowledgeable individuals from cross functional departments that reviews, approves and manages changes to configuration items.
> b. Ensure that the oversight body formed in 'a' above, develops a configuration management plan that documents roles and responsibilities, configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's software development life cycle; performing configuration monitoring; and applying configuration management requirements to contracted systems. The plan should also ensure that the originator and approver of changes are not the same persons.

IAF Needs to Test the Foundation's Continuity of Operations Plan

NIST SP 800-53, Rev. 4, security control, CP-4 Contingency Plan Testing, states:

> The organization:
>
> a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
> b. Reviews the contingency plan test results; and
> c. Initiates corrective actions, if needed.

In addition, security control CP-2(8), Contingency Plan | Identify Critical Assets, states:

> The organization identifies critical information system assets supporting essential missions and business functions. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses.

To ensure that essential services are available in natural or manmade emergencies--such as terrorist attacks, severe weather, or building-level emergencies--federal agencies are required to develop, implement, and test a continuity of operations plan.

IAF has developed, but not tested its continuation of operations plan and documented the result of the test for Fiscal Year (FY) 2018. IAF's management stated that the reason for not testing the continuation of operations plan was due to "prioritizing resources to initiate and complete a significant infrastructure project whereby all physical production servers were migrated to virtual servers. Given the low risks [of cloud services] and magnitude of impact to the production environment, staff resources were dedicated to ensuring a migration without any production down time, which was achieved as of June 2018."

IAF will be at risk if an incident occurs that requires the implementation of a continuity of operations plan that has not been tested for effectiveness, thus jeopardizing the ability of the IAF to continue its essential operations.

> **Recommendation 3:** We recommend that the Inter-American Foundation's Chief Information Officer test and exercise the Foundation's Continuity of Operations Plan and document the specific test and exercise activities conducted with their results.

IAF Needs to Mitigate Network Vulnerabilities

NIST SP 800-53, Rev. 4, security control, SI-2, states the following regarding flaw remediation:

> The organization:
>
> a. Identifies, reports, and corrects information system flaws.
> * * *
> c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

IAF had a process in place to remediate vulnerabilities within patch cycles. Additionally, IAF has corrected some of the prior year patch management vulnerabilities related to out-of-commissioned 2013 servers. However, FY 2018 independent scans performed using Qualys confirmed 3 "Urgent," 3 "Critical," and 65 "Serious" level risk vulnerabilities related to patch and configuration management.

IAF has implemented patch management procedures; however, controls were not consistently implemented to remediating known vulnerabilities. Unmitigated vulnerabilities on IAF's network can compromise the confidentiality, integrity, and availability of IAF data. For example:

- An attacker may leverage known issues to execute arbitrary code.
- Foundation employees may be unable to access systems.
- Foundation data may be compromised.

Recommendation 4: We recommend that the Inter-American Foundation's Chief information Officer 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.

IAF Needs to Implement Multi-factor Authentication

NIST Special Publication 800-53, Revision 4, security control IA-2, states the organization should implement multifactor authentication for privileged and non-privileged accounts to gain access to the information system.

In addition, Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and* Contractors (August 27, 2004) requires the use of Personal Identification Verification for gaining logical access to federally controlled information systems.

IAF did not implement multifactor authentication for its privileged and non-privileged users. Multifactor authentication was only implemented for remote access.

By not fully implementing multifactor authentication, IAF increases the risk that unauthorized individuals could gain access to its information system and data.

A recommendation addressing this finding was issued in the fiscal year 2016 FISMA audit[4]. IAF purchased equipment capable of accepting Personal Identify Verification (PIV) cards and has obtained the application patches necessary to require PIV card enabled authentication for all its systems. However, IAF has not implemented the patch fully to remediate the control weakness. Therefore, we are not making recommendation related to this control weakness at this time.

[4] The Inter-American Foundation has Implemented Many Controls in Support of FISMA, but Improvements are Needed (Audit Report No. A-IAF-17-004-C, November 7, 2016).

Evaluation of Management Comments

In response to the draft report, the Inter-American Foundation described planned actions to address all four recommendations. IAF agreed with recommendations 1, 3 and 4, and partially concurred with recommendation 2. In regard to recommendation 2, IAF agreed to articulate its change control structure, but did not believe creating a change control board would reduce their overall risks and prepared a formal memo to accept the risk of not having a change control board. IAF's comments are included in their entirety in Appendix III.

Based on our evaluation of management comments, we acknowledge management decisions on all four recommendations.

Scope and Methodology

Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether IAF implemented selected security controls for certain information systems[5] in support of the Federal Information Security Modernization Act of 2014.

Our overall objective was to evaluate IAF's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of IAF's Information Technology (IT) security program in accordance with U.S. Department of Homeland Security's (DHS) FISMA Inspector General reporting requirements:

- Risk Management;
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of IAF's IT security governance structure and the Foundation's system security assessment and authorization (SA&A) methodology. We also followed-up on outstanding recommendations from prior FISMA audits (see Appendix II), and performed audits focused on IAF's major information systems. The audit also included a vulnerability assessment of an IAF-managed system and an evaluation of IAF's process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed IAF's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also audited an internal system and IAF's SA&A process. We considered the internal control structure for IAF's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over IAF's sole internally-managed system and 2 out of a population of 9 other contractor-owned and managed systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When

[5] See Appendix IV for a list of controls selected.

appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to IAF's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the FY 2017 FISMA audit report; and
- Completed a network vulnerability assessment of IAF's sole internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for IAF's systems taken as a whole.

The criteria used in conducting this audit included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- NIST SP 800-12, Revision 1, *An Introduction to Computer Security*: The NIST Handbook;
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors and*
- Other criteria as appropriate.

The audit was conducted at IAF's headquarters in Washington, D.C., from April 17, 2018 through September 6, 2018.

Status of Prior Year Findings

No.	FY 2017[6] and 2016[7] Audit Recommendations	Status	Auditor's Position on Status
1	**FY 2017 FISMA audit recommendation No. 1**: *"We recommend that the Inter-American Foundation's Chief Information Officer remediate unsupported software and configuration related vulnerabilities in the network identified by the Office of Inspector General's contractor, as appropriate, and document the results or document acceptance of the risks of those vulnerabilities."*	Open	Agree
2	**FY 2017 FISMA audit recommendation No. 2**: *"We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test system changes and document the results of testing."*	Closed	Agree
3	**FY 2017 FISMA audit recommendation No. 3**: *"We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test the Foundations incident response capabilities."*	Closed	Agree.
4	**FY 2016 FISMA audit recommendation No. 5**: *"Inter-American Foundation's Chief Information Officer obtain a current authorization to operate the Enterprise Network system that results from a completed security controls assessment and updated system security plan, risk assessment, and plan of action and milestones."*	Closed	Agree
5	**FY 2016 FISMA audit recommendation 7**: "*We recommend that the Inter-American Foundation's Chief Information Officer implement multifactor authentication for all network accounts and document the results."* (Audit Report No. A-IAF-17-004-C, November 7, 2016)	Open	Agree Noncompliance with FIPS PUB 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors

[6] *The Inter-American Foundation has Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements are Needed* (Audit Report No. A-IAF-18-002-C, October 2, 2017).
[7] *The Inter-American Foundation has Implemented Many Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-IAF-17-004-C, November 7, 2016).

No.	FY 2017[6] and 2016[7] Audit Recommendations	Status	Auditor's Position on Status
6	**FY 2016 FISMA audit recommendation 8**: *"We recommend that the Inter-American Foundation's Chief Information Officer update the continuity of operations plan to include a business impact analysis."*	Open (Partially resolved)	Agree IAF updated its plan but did not perform Business Impact Analysis

Management Comments

(Excluding Attachment)

Inter-American Foundation
An Independent Agency of the U.S. Government

October 5, 2018

MEMORANDUM

TO: Mark Norman, Director, IG/A/ITA, USAID OIG

CC: Lesley Duncan, Chief Operating Officer, Inter-American Foundation

FROM: Rajiv Jain, Chief Information Officer, Inter-American Foundation /s/ Rjain

SUBJECT: Plan and Action on Recommendations from USAID OIG Audit Report No. A-IAF-18-00X-C dated September 26, 2018

This memorandum provides actions planned to address the recommendations contained in the Audit of the Inter-American Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2018, Audit Report A-IAF- 18-00X-C dated September 26, 2018.

Recommendation 1: We recommend that the Inter-American Foundation's Chief Information Officer develop and implement an enterprise risk management policy that fully defines the Foundation's risk management policies, procedures, and strategy, including (a) the organization's processes and methodologies for categorizing risk; (b) developing a risk profile; (c) assessing risk and risk appetite/tolerance levels and responding to risk; and (d) monitoring risk.

In response to Recommendation 1, IAF proposes the following actions to mitigate the finding:

1. The IAF will develop an updated enterprise risk management policy consistent with federal requirements and the agency's risk strategy. Procedures will be developed to define methodologies for categorizing risk.
2. The IAF will annually review and adjust the risk profile with inputs taken from assessments and other defined indicators of risk.

Target date: 6/30/2019

Recommendation 2: We recommend that the Inter-American Foundation's Chief Information Officer:

a. Create a Change Control Board (CCB) or related oversight body, composed of knowledgeable individuals from cross functional departments that reviews, approves and manages changes to configuration items.

b. Ensure that the oversight body formed in 'a' above, develops a configuration management plan that documents roles and responsibilities, configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's software development life cycle; performing configuration monitoring; and applying configuration management requirements to contracted systems. The plan should also ensure that the originator and approver of changes are not the same persons.

In response to Recommendation 2, IAF partially concurs with the recommendation and agrees to articulate our Change Control Structure, primarily:

- The IAF is a small agency of less than 50 personnel with a small IT footprint. Core services are hosted on third party cloud environments and business-enabling systems are supported by third-party vendors. The IAF reviews the performance of IT support contracts annually.

- In practice, all requests for change are reviewed by the CIO and CISO and requests for new systems are also reviewed by the COO. Business and technical requirements are formally defined and changes are made accordingly, ensuring separation of duties between developers and those responsible for migrating changes.

- The IAF has submitted a formal risk acceptance memo. The IAF does not believe creating a CCB at IAF will reduce the overall risks, given the risk tolerance of the agency combined with compensating controls and mitigating controls as noted above.

Target date: 12/30/2018
Attached: Risk acceptance memo

Recommendation 3: We recommend that the Inter-American Foundation's Chief Information Officer test and exercise the Foundation's Continuity of Operations Plan and document the specific test and exercise activities conducted with their results.

In response to Recommendation 3, IAF proposes the following actions to mitigate the finding:

1. The IAF will perform an annual COOP exercise, document the results, identify lessons learned and take action on items requiring follow-up.

Target date: 3/30/2019

Recommendation 4: We recommend that the Inter-American Foundation's Chief information Officer 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 response to Recommendation 4, IAF proposes the following actions to mitigate the finding:

1. The IAF will update the Standard Operating Procedures (SOP) to define remediation time of vulnerabilities based on risk.
2. The IAF will continue to conduct scans twice a quarter, and review, evaluate and close open configuration-related vulnerabilities identified from scans and other sources such as DHS and OMB directives.
3. Closures of vulnerabilities will be formally documented and reviewed; any risks accepted will be supported by a business justification.

Target date: 3/30/2019

Number of Controls Reviewed for Each System

Control No.	Control Name	Number of Systems Tested
AC-1	Access Control Policy & Procedures	1
AC-2	Account Management	3
AC-8	System Use Notification	1
AC-17	Remote Access	1
AC-20	Use of External Information Systems	1
AT-1	Security Awareness & Training Policy and Procedures	1
AT-2	Security Awareness	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policy & Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	3
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	1
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policy & Procedures	1
CM-2	Baseline Configuration	1
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	1
CM-9	Configuration Management Plan	1
CM-10	Software Usage Restrictions	1
CP-1	Contingency Planning Policy & Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing and Exercises	1
CP-6	Alternate Storage Sites	1
CP-7	Alternate Processing Sites	1
CP-8	Telecommunication Services	1
CP-9	Information System Backup	1

Control No.	Control Name	Number of Systems Tested
IA-1	Identification & Authentication Policy and Procedures	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
PL-2	System Security Plan	1
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	1
PM-6	Information Security Measures of Performance	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PM-11	Mission/Business Process Definition	1
PS-1	Personnel Security Policy & Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	3
SA-3	System Development Life Cycle Support	3
SA-4	Acquisitions Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	2
SI-2	Flaw Remediation	1
SI-4	Information System Monitoring	1
SE-1	Inventory of Personally Identifiable Information	1
SE-2	Privacy Incident Response	1
DM-1	Minimization of Personally Identifiable Information	1
DM-3	Minimization of PII Used in Testing, Training, and Research	1
AR-5	Privacy Awareness and Training	1
SC-28	Protection of Information at Rest	1
SC-7	Boundary Protection	1
	TOTAL CONTROLS	**72**

Acronyms

Acronyms	
CCB	Change Control Board
CM	Configuration Management
COOP	Continuity of Operations
CP	Contingency Plan
DHS	U.S. Department of Homeland Security
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IG	Inspector General
IAF	Inter-American Foundation
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PUB	Publication
SA&A	Security Assessment and Authorization
SOP	Standard Operating Procedures
SP	Special Publication