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

IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019

AUDIT REPORT A-IAF-20-004-C
JANUARY 23, 2020

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

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, Millennium Challenge Corporation, U.S. African Development Foundation, Inter-American Foundation, 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: January 23, 2020

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 2019 (A-IAF-20-004-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2019. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct the audit. The contract required Brown & Company to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Brown & Company's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed 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 & Company is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Brown & Company did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether IAF implemented an effective information security program.[1] To answer the audit objective, the audit firm tested selected management, technical, and operational controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Brown & Company reviewed IAF's three major information systems. Fieldwork took place at IAF's headquarters in Washington, DC, from May 29, 2019, through November 6, 2019. It covered the period from October 1, 2018, through September 30, 2019.

[1] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

The audit firm concluded that IAF generally implemented an effective information security program by implementing 78 of 89 selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of IAF's information and information systems. For example, IAF:

- Improved documentation of its risk management policy, procedures, and strategy;
- Established an organization structure to improve the process for reviewing, approving, and documenting configuration management changes;
- Conducted a table-top exercise to test its Continuity of Operations Plan (COOP) to ensure the availability and effectiveness of the plan; and
- Updated its Enterprise Risk Management controls and Configuration Management Plan.

However, as summarized in the table below, Brown & Company noted weaknesses in four of the eight FISMA metric domains. The weaknesses occurred because IAF did not implement 11 controls related to maintaining an accurate system inventory, preparing a business impact analysis, providing specialized security training, and fully implementing multi-factor authentication. With these weaknesses, IAF's information and information systems are potentially exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2019 IG FISMA Metric Domains[2]	**Weaknesses Identified**
Risk Management	X
Configuration Management	
Identity and Access Management	X
Data Protection and Privacy	
Security Training	X
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	X

The weakness related to multi-factor authentication was raised in previous years. Since a recommendation to address the issue was made previously and has not been closed, we are not repeating it in this report. To address the other weaknesses identified in the report, we recommend that IAF's chief information officer:

Recommendation 1: Develop and implement procedures for maintaining an accurate hardware and software inventory in accordance with NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," Security

[2] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 9, 2019.

Control CM-8, information system component inventory, and IAF's standard operating procedures.

Recommendation 2: Update the Continuity of Operations Plan to include a business impact analysis.

Recommendation 3: Enforce policies and procedures to ensure that specialized security training is provided to and completed by all privileged users with significant security responsibilities in FY 2020.

In finalizing the report, Brown & Company evaluated IAF's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1, 2, and 3 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 & Company's employees during the engagement.

The Inter-American Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019

Final Report

December 12, 2019

Prepared by
Brown & Company CPAs and
Management Consultants, PLLC
6401 Golden Triangle Dr., Suite 310
Greenbelt, MD 20770

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 or Foundation) 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 2019*. 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 an effective information security program. For this audit, an effective information security program was defined as implementing certain security controls for selected 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 three major 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 IAF's headquarters in Washington, D.C., from May 29, 2019, through November 6, 2019.

Our audit was performed in accordance with the performance audit standards specified in *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.

We concluded that IAF generally implemented an effective information security program by implementing many selected security controls for selected information systems. Although IAF generally implemented an effective information security program, its implementation of certain 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 three recommendations to assist IAF in strengthening its information security program. In addition, one recommendation from prior years was not fully implemented, and therefore, a new recommendation was 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

Brown & Company
Greenbelt, Maryland
December 12, 2019

The Inter-American Foundation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019

Table of Contents

Page

BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Summary of Results

The United States Agency for International Development (USAID) Office of Inspector General (OIG) engaged 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 an effective[1] information security program.

The Federal Information Security Modernization Act of 2014[2] (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems[3], 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.

The statute also provides a mechanism for improved oversight of Federal Agency information security programs. FISMA 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.

Our audit was performed in accordance with generally accepted government auditing standards (GAGAS). 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 objective.

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

[1] For this audit, an effective security program was defined as implementing certain security controls for selected information systems in support of FISMA.

[2] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002.

[3] 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 implemented an effective information security program by implementing 78 of 89[4] selected security controls for selected information systems. For example, IAF:

- Improved documentation of its risk management policy, procedures, and strategy;
- Established an organization structure to improve the process for reviewing, approving and documenting configuration management changes;
- Conducted a table-top exercise to test its Continuity of Operations Plan (COOP) to ensure the availability and effectiveness of the plan; and
- Updated the IAF's Enterprise Risk Management controls and Configuration Management Plan.

Although IAF generally implemented an effective information security program, its implementation of 11 of the 89 selected security 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. Specifically, IAF needs to:

- Maintain an accurate and complete record of its information system hardware and software inventory;
- Prepare a business impact analysis;
- Ensure that specialized security training is provided to privileged users; and
- Implement multi-factor authentication for non-privileged accounts.

As a result, we noted weaknesses in the following FY 2019 IG FISMA Metric Domains:

Cybersecurity Framework Security Functions[5]	FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Identify	Risk Management	IAF needs to maintain an accurate and complete information system hardware and software inventory.

[4] There were 67 NIST SP 800-53, Revision 4, controls specifically identified in the FY 2019 IG metrics. We tested the 64 controls that were applicable to systems within the scope of our audit. We also tested 2 additional privacy controls from Appendix J of NIST SP 800-53 Revision 4 because they related to the metrics. A control was counted for each system it was tested against. Thus, there were 89 instances of testing a control. See Appendix III for the Number of Controls Reviewed for Each System.
[5] NIST Cybersecurity Framework Version 1.1(April 2018).

Cybersecurity Framework Security Functions[5]	FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Protect	Configuration Management	No weakness identified.
	Identity and Access Management	IAF needs to implement multi-factor authentication for non-privileged accounts.
	Data Protection and Privacy	No weakness identified.
	Security Training	IAF needs to ensure that specialized security training is provided to privileged users.
Detect	Information Security Continuous Monitoring	No weakness identified.
Respond	Incident Response	No weakness identified.
Recover	Contingency Planning	IAF needs to prepare a Business Impact Analysis.

Therefore, IAF's operations and assets may be at risk of unauthorized access, misuse and disruption. This report makes three recommendations to assist IAF in strengthening its information security program. In addition, as illustrated in Appendix II, Status of Prior Year Findings, 1 of 6 prior year recommendations had not yet been fully implemented, and therefore, a new recommendation was not made. Detailed findings appear in the following section.

Audit Findings

IAF Needs To Maintain An Accurate And Complete Information System Hardware And Software Inventory

Cybersecurity Framework Security Function: *Identify*
FY 19 FISMA IG Metric Domain: *Risk Management*

NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4), Security *and Privacy Controls for Federal Information Systems and Organizations*, Security Control CM-8, Information System Component Inventory states the following regarding system inventories:

> The organization:
>
> a. Develops and documents an inventory of information system components that:
>   1. Accurately reflects the current information system;
>   2. Includes all components within the authorization boundary of the information system;
>   3. Is at the level of granularity deemed necessary for tracking and reporting;
>
>   ***
>
> b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

IAF's *Information System Security Program, Standard Operating Procedures*, March 2019, states, "information system updates the inventory of information system components during installation, removals, and information system updates."

We obtained and reviewed the IAF software and hardware inventory schedule. IAF manually maintains an inventory of servers, databases, network devices, software, etc. on a "Master Inventory" schedule, but it does not have accurate and complete records. The "Master Inventory" lists the devices and software that reside within the environment, but it does not describe the specific servers that the software reside on, or the information systems the devices and software support. The various elements of an inventory should be mapped to each other so that IAF can accurately define the boundaries of its information systems.

During our audit inspection of 11 judgmentally selected IT hardware devices from a population of 154, we noted five exceptions: two devices could not be located, two devices did not have serial numbers recorded, and one device had the wrong IP address recorded. This occurred because IAF did not have procedures for maintaining an accurate hardware and software inventory.

The lack of an accurate, complete and updated system inventory significantly hinders

IAF's efforts related to management oversight, risk management, and securing the agency's information systems.

> **Recommendation 1:** We recommend that IAF's Chief Information Officer develop and implement procedures for maintaining an accurate hardware and software inventory in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Control CM-8, Information System Component Inventory, and IAF's Standard Operating Procedures.

IAF Needs To Update The Continuity Of Operations Plan To Include A Business Impact Analysis

Cybersecurity Framework Security Function: *Recover*
FY 19 FISMA IG Metric Domain: *Contingency Planning*

NIST SP 800-53, Rev. 4, Security Control CP-2, Contingency Plan states the following regarding contingency planning:

> The organization:
>
> a. Develops a contingency plan for the information system that: ***
>
>   2. Provides recovery objectives, restoration priorities, and metrics; ***
>   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
>   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

IAF's Continuity of Operations Plan (COOP) dated February 2017 did not include a business impact analysis. Specifically, the COOP did not fully address maintaining business functions, which would be addressed in the business impact analysis. IAF's business impact analysis should be an analysis of its IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. Due to limited resources and competing priorities, IAF did not conduct the business impact analysis.

Without a complete contingency plan, IAF is at risk of not being able to adequately return to its business operations after an emergency or natural disaster. Additionally, lack of a complete and accurate contingency plan increases the likelihood that the contingency plans in place will not function appropriately.

> **Recommendation 2:** We recommend that IAF's Chief Information Officer update the continuity of operations plan to include a business impact analysis.

IAF Needs To Ensure That Specialized Security Training Is Provided To Privileged Users

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Security Training*

NIST SP 800-53, Rev. 4, Security Control AT-3 Role-Based Security Training states the following regarding specialized security training:

> The organization provides role-based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes;
> c. [Assignment: organization-defined frequency] thereafter.

During the audit, we interviewed IAF's Chief Information Officer, Chief Information Security Officer, and specialized IT contractors and consultants to document their access to and completion of role-based security training as it relates to implementing IAF's information system security controls.

For 7 privileged users with security roles and responsibilities, 2 had not completed role-based security training in FY 2019. This occurred because IAF had other competing priorities for these personnel.

By not ensuring that specialized security training was provided to and completed by all privileged users with significant security responsibilities at IAF in FY 2019, IAF increased the likelihood that key personnel with assigned security roles and responsibilities may not have the requisite specialized training to: identify, isolate, and mitigate the risks associated with IT threat and vulnerabilities, which may adversely impact the confidentiality, integrity, and availability of IAF mission critical systems and high value assets.

> **Recommendation 3:** We recommend that IAF's Chief Information Officer enforce policies and procedures to ensure that specialized security training is provided to and completed by all privileged users with significant security responsibilities in FY 2020.

IAF Needs To Implement Multi-Factor Authentication For Non-Privileged Accounts

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Rev. 4, Security Control IA-2, Identification And Authentication (Organizational Users), states the following regarding multi-factor authentication:

> The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
>
> Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication.

U.S. Office of Management and Budget (OMB) Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12*, requires IAF to use Personal Identity Verification (PIV) credentials for multi-factor authentication by the beginning of FY 2012. In addition, the memorandum stated that all new systems under development must be PIV compliant prior to being made operational.

IAF has IT equipment capable of accepting PIV cards. However, IAF has not implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access IAF's networks and systems. Multifactor authentication for non-privileged users was only implemented for remote access. IAF is not fully PIV compliant until all of its information systems (applications) can be accessed only via PIV authentication in lieu of a username and password. Due to limited resources and competing priorities, IAF has not employed sufficient resources to fully comply with OMB M-11-11.

By not fully implementing multifactor authentication, IAF increases the risk that unauthorized individuals could gain access to its information system and data. This is a critical control because without PIV authentication enforced at the application level, users of the network (either authorized or unauthorized) could still gain access to applications that they are not authorized to use, and public-facing systems are more vulnerable to remote attack.

A recommendation addressing this finding was issued in the fiscal year 2016 FISMA audit. Since that recommendation is still open, we are not making a new recommendation at this time.

Evaluation of Management Comments

We provided our draft report to the Inter-American Foundation on November 27, 2019, and on December 11, 2019, received its response, which is included as Appendix III. The report includes three recommendations and we acknowledge management decisions on all three. We consider the three recommendations open pending completion and evaluation of planned actions.

Appendix I – Scope and Methodology

Scope

We conducted this audit in accordance with GAGAS, 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 an effective information security program.

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 fieldwork focused on three 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.

The audit was conducted at IAF's headquarters in Washington, D.C., from May 29, 2019 through November 6, 2019. It covered the period from October 1, 2018, through September 30, 2019.

Methodology

We reviewed IAF's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. 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 appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish the 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;
- Reviewed IAF's SA&A process;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the FY 2018 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 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security*: The NIST Handbook;
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 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, Rev. 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.

Appendix II – Status of Prior Year Findings

No.	FY 2018[6], FY 2017[7] and 2016[8] Audit Recommendations	IAF Position On Status	Auditor's Position on Status
1	**FY 2018 FISMA audit recommendation No. 1:** "*We recommend that the Inter-American Foundation's Chief Information Officer develop and implement an enterprise risk management (ERM) 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.*"	Closed	Agree
2	**FY 2018 FISMA audit recommendation No. 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*	Closed	Agree

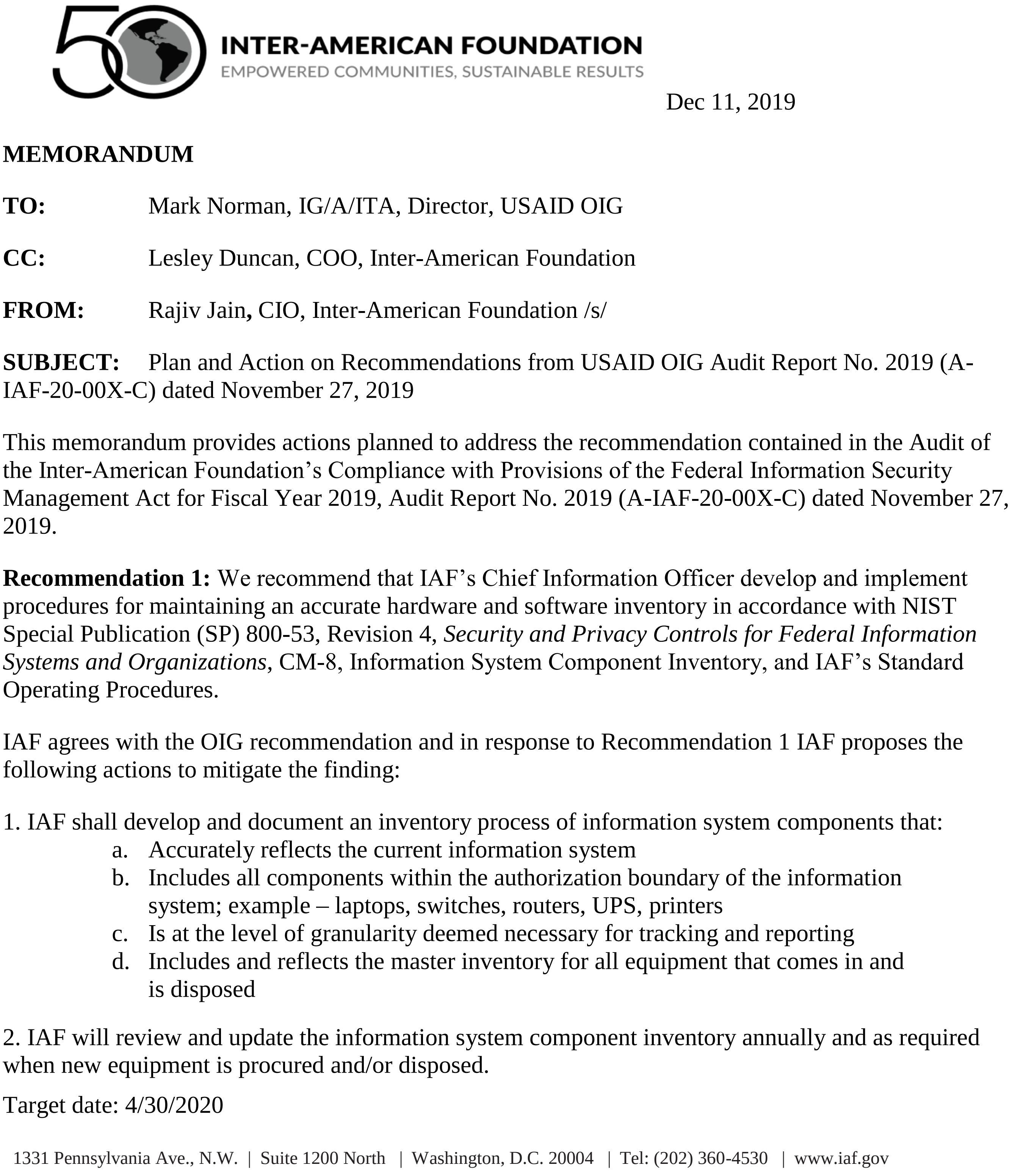
[6] *The Inter-American Foundation has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (Audit Report No. A-IAF-19-003-C, November 2, 2018).*

[7] *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).

[8] *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 2018[6], FY 2017[7] and 2016[8] Audit Recommendations	IAF Position On Status	Auditor's Position on Status
	same persons."		
3	**FY 2018 FISMA audit recommendation No. 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."*	Closed	Agree
4	**FY 2018 FISMA audit recommendation No. 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*."	Closed	Agree
5	**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."*	Closed	Agree
6	**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 See finding 4.

Appendix III – Management Comments



INTER-AMERICAN FOUNDATION
EMPOWERED COMMUNITIES, SUSTAINABLE RESULTS

Dec 11, 2019

MEMORANDUM

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

CC: Lesley Duncan, COO, Inter-American Foundation

FROM: Rajiv Jain**,** CIO, Inter-American Foundation /s/

SUBJECT: Plan and Action on Recommendations from USAID OIG Audit Report No. 2019 (A-IAF-20-00X-C) dated November 27, 2019

This memorandum provides actions planned to address the recommendation contained in the Audit of the Inter-American Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2019, Audit Report No. 2019 (A-IAF-20-00X-C) dated November 27, 2019.

Recommendation 1: We recommend that IAF's Chief Information Officer develop and implement procedures for maintaining an accurate hardware and software inventory in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CM-8, Information System Component Inventory, and IAF's Standard Operating Procedures.

IAF agrees with the OIG recommendation and in response to Recommendation 1 IAF proposes the following actions to mitigate the finding:

1. IAF shall develop and document an inventory process of information system components that:
    a. Accurately reflects the current information system
    b. Includes all components within the authorization boundary of the information system; example – laptops, switches, routers, UPS, printers
    c. Is at the level of granularity deemed necessary for tracking and reporting
    d. Includes and reflects the master inventory for all equipment that comes in and is disposed

2. IAF will review and update the information system component inventory annually and as required when new equipment is procured and/or disposed.

Target date: 4/30/2020

Recommendation 2: We recommend that IAF's Chief Information Officer update the continuity of operations plan to include a business impact analysis.

IAF agrees with the OIG recommendation and in response to Recommendation 2 IAF proposes the following action to mitigate the finding:

1. IAF shall develop a contingency plan for the information system that:
    a. Provides recovery objectives, restoration priorities, and metrics;
    b. Addresses maintaining essential mission and business functions despite an information system disruption, compromise, or failure;
    c. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

Target date: 5/30/2020

Recommendation 3: We recommend that IAF's Chief Information Officer enforce policies and procedures to ensure that specialized security training is provided to and completed by all privileged users with significant security responsibilities in FY 2020.

IAF agrees with the OIG recommendation and in response to Recommendation 3, IAF proposes the following action to mitigate the finding:

1. IAF shall provide role-based security training to personnel with assigned security roles and responsibilities:
    a. Before authorizing access to the information system or performing assigned duties
    b. When required by major information system changes
    c. The role based training shall be required annually thereafter.

Target date: 4/30/2020

Appendix IV – Number of Controls Reviewed for Each System

Control No.	Control Name	Number of Systems Tested
AC-1	Access Control Policy & Procedures	2
AC-2	Account Management	2
AC-8	System Use Notification	1
AC-17	Remote Access	2
AR-1	Governance and Privacy Program	2
AR-2	Privacy Impact and Risk Assessment	2
AR-4	Privacy Monitoring and Auditing	2
AR-5	Privacy Awareness and Training	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	2
CA-3	System Interconnections	2
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	2
CA-7	Continuous Monitoring	2
CM-1	Configuration Management Policy & Procedures	1
CM-2	Baseline Configuration	2
CM-3	Configuration Change Control	2
CM-6	Configuration Settings	2
CM-7	Least functionality	2
CM-8	Information System Component Inventory	2
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
IA-1	Identification & Authentication Policy and Procedures	2
IR-1	Incident Response Policy & Procedures	1

APPENDIX IV

Control No.	Control Name	Number of Systems Tested
IR-4	Incident Handling	1
IR-6	Incident Response Assistance	1
IR-7	Incident Reporting	1
MP-3	Media Marking	1
MP-6	Media Sanitization	1
PL-2	System Security Plan	2
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	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	2
SA-4	Acquisitions Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	2
SC-8	Transmission Confidentiality and Integrity	1
SC-28	Protection of Information at Rest	1
SI-2	Flaw remediation	2
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-7	Software, Firmware, and Information Integrity	1
SE-2	Privacy Incident Response	2
	TOTAL CONTROLS	**89**

Appendix V – Glossary

Acronyms	
CCB	Change Control Board
CM	Configuration Management
COOP	Continuity of Operations 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
GAGAS	Generally Accepted Government Auditing Standards
IA	Identification and Authentication
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
RA	Risk Assessment
Rev.	Revision
SA	Security Architecture
SA&A	Security Assessment and Authorization
SP	Special Publication