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

# IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA

**AUDIT REPORT A-IAF-21-002-C**
**DECEMBER 4, 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, and Inter-American Foundation.

## 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: December 4, 2020

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

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

SUBJECT: IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA (A-IAF-21-002-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF) information security program for fiscal year 2020 in support of the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates LLC (RMA) to conduct the audit. The contract required RMA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed RMA'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. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which RMA 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, RMA tested IAF's implementation of selected 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." RMA auditors reviewed five of the seven information systems in IAF's inventory dated July 2020. Fieldwork covered IAF's headquarters in Washington, DC, from April 24 to

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

September 10, 2020. It covered the period from October 1, 2019, through September 10, 2020.

The audit firm concluded that IAF generally implemented an effective information security program by implementing 87 of 100[2] selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the Agency's information and information systems. Among those controls, IAF maintained:

- an effective process for assessing the risk associated with positions involving information system duties.
- an effective security awareness training program that included role-based training for positions with elevated information system permissions.
- an accurate inventory of hardware and software assets.

However, as summarized in the table below, RMA noted weaknesses in all eight FISMA metric domains. The weaknesses were mostly due to policy and procedures not being reviewed and updated in a timely manner in all domains, with additional weaknesses identified in IAF's Risk Management, Identity and Access Management, and Contingency Planning domains. With these weaknesses, RMA concluded that IAF's controls were not fully effective in preserving the confidentiality, integrity, and availability of the agency's information and information systems.

| **Fiscal Year 2020<br>IG FISMA Metric Domains[3]** | **Weaknesses Identified** |
|---|---|
| Risk Management | X |
| Configuration Management | X |
| Identity and Access Management | X |
| Data Protection and Privacy | X |
| Security Training | X |
| Information Security Continuous Monitoring | X |
| Incident Response | X |
| Contingency Planning | X |

To address the weaknesses identified in RMA's report, we recommend that IAF's Chief Information Officer take the following actions:

**Recommendation 1.** Develop and implement policies and procedures related to Plan of Action and Milestones to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to

[2] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the fiscal year 2020 IG metrics. RMA tested 86 controls. A control was counted for each system it was tested against. Thus, there were 100 instances of testing a control.

[3] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," (April 17, 2020).

extend estimated completion dates and determine the dependencies and completion of milestones that affect the estimated due dates to ensure that they are met.

**Recommendation 2.** Create a monitoring plan to review and update policies and procedures in accordance with the timeliness requirements established in agency policies.

In addition, IAF has not taken final corrective action on two recommendations made in our 2016[4] and 2019[5] FISMA audit reports regarding weaknesses in the Identity and Access Management, and Contingency Planning domains. See Appendix II on page 12 of RMA's report for the full text of those two recommendations.

In finalizing the report, the audit firm evaluated IAF's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

[4] Recommendation 7 in USAID OIG, "The Inter-American Foundation Has Implemented Many Controls in Support of FISMA But Improvements are Needed" (A-IAF-17-004-C), November 7, 2016.

[5] Recommendation 2 in USAID OIG, "IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019" (A-IAF-20-004-C), January 23, 2020.

RMA Associates

Auditors. Consultants. Advisors.

# Inter-American Foundation (IAF)

## Federal Information Security Modernization Act of 2014 (FISMA)

Final Report

FY 2020

RMA | Associates
Auditors. Consultants. Advisors.

December 4, 2020

Mr. Mark 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:

RMA Associates, LLC (RMA) is pleased to present our report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year (FY) 2020.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and that of IAF. We will be happy to answer any questions you may have concerning the report.

Reza Mahbod

Respectfully,
Reza Mahbod, CPA, CISA, CFE, CGFM, CICA, CGMA, CDFM, CDPSE
President
RMA Associates, LLC

RMA | Associates
Auditors. Consultants. Advisors.

Inspector General
United States Agency for International Development
Washington, D.C.

December 4, 2020

RMA Associates, LLC (RMA) conducted a performance audit of the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether IAF implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated January 22, 2015.

For this audit, we reviewed selected controls from five of IAF's seven information systems. Audit fieldwork covered IAF's headquarters located in Washington, D.C., from April 24, 2020, to September 10, 2020.

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 objective.

We concluded that IAF generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. However, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in all eight Inspector General (IG) FISMA Metric Domains mostly due to policy and procedures not being reviewed within IAF's defined frequency. We made two recommendations to assist IAF in strengthening its information security program. In addition, two findings related to prior year recommendations are still open.

Additional information on our findings and recommendations are included in the accompanying report.

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

**Table of Contents**

## Summary of Results

### Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual evaluation of the Inter-American Foundation's (IAF) information security program. The objective of this performance audit was to determine whether IAF implemented an effective[2] information security program.

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other sources. Because IAF 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 (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 OMB and congressional committees on the effectiveness of their information security program.

FISMA also requires agency IGs to assess the effectiveness of agency information security programs and practices to determine the effectiveness of such program and practices, and to report the results of the assessments to the Office of Management and Budget (OMB).

Annually, OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for assessing agency information security programs. On November 19, 2019, OMB issued OMB Memorandum M-20-04, "*Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*." According to that memorandum, each year, the IGs are required to complete metrics[3] to independently assess their agencies' information security programs.

[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 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

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

[3] The IG FISMA metrics will be completed as a separate deliverable.

The FY 2020 metrics are designed to assess the maturity[4] of an information security program and align with the five functional areas in the NIST Cybersecurity Framework, Version 4.0: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

*Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2020 IG FISMA Metric Domains*

| Cybersecurity Framework Security Functions | FY 2020 IG FISMA Metric Domains |
|---|---|
| Identify | Risk Management |
| Protect | Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training |
| Detect | Information Security Continuous Monitoring |
| Respond | Incident Response |
| Recover | Contingency Planning |

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Results

The audit concluded that IAF generally implemented an effective information security program by implementing 87 of 100[5] instances of security controls. For example, IAF:

- Maintained an effective process for assessing the risk associated with positions involving information system duties;
- Maintained an effective security awareness training program that includes role-based training for positions with elevated information system permissions; and
- Maintained an accurate inventory of hardware and software assets.

Although IAF generally implemented an effective information security program, its implementation of 13 of 100 instances of selected controls was not fully effective in preserving the confidentiality, integrity, and availability of the agency's information and information systems. As a result, we noted weaknesses in all eight IG FISMA Metric Domains (Table 2) and presented recommendations to assist the agency in strengthening its information security program. One weakness applied to all domains.

[4] The five maturity models include: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.

[5] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested 86 controls. A control was counted for each system it was tested against. Thus, there were 100 instances of testing a control. See Appendix III for a list of the controls.

*Table 2: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2020 FISMA Assessment*

| Cybersecurity Framework Security Functions | FY 2020 IG FISMA Metric Domains | Weakness Noted in FY 2020 |
|---|---|---|
| Identify | Risk Management | IAF Needs to Accurately Document and Remediate Plan of Action and Milestone (POA&Ms) (Finding 1).<br>IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| Protect | Configuration Management | IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| | Identity and Access Management | IAF Needs to Periodically Review Policy and Procedures (Finding 2).<br>IAF Needs to Implement Multi-Factor Authentication for Non-Privileged Accounts (Finding 4). |
| | Data Protection and Privacy | IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| | Security Training | IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| Detect | Information Security Continuous Monitoring | IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| Respond | Incident Response | IAF Needs to Periodically Review Policy and Procedures (Finding 2). |
| Recover | Contingency Planning | IAF Needs to Periodically Review Policy and Procedures (Finding 2).<br>IAF Needs to Update the Continuity of Operations Plan to Include a Business Impact Analysis (Finding 3). |

In addition, as illustrated in Appendix II, Status of Prior Year Findings, two of four prior year recommendations had not yet been fully implemented, and therefore, new recommendations were not made to address those weaknesses.  Detailed findings appear in the following section.

## Audit Findings

### 1. IAF Needs to Accurately Document and Remediate Plans of Action and Milestones (POA&Ms).

**Cybersecurity Framework Security Function:** *Identify*
**FY20 IG FISMA Metric Domain:** *Risk Management*

IAF identifies and tracks weaknesses at the enterprise-level, as well as tracks system-specific weaknesses at the system-level. However, IAF did not document and accurately record relevant information in the POA&M Register. We found IAF did not assign criticality to each POA&M. Also, there were scheduled completion dates missing, a lack of an overall remediation plan, inconsistencies, and incomplete records in the POA&M Register.

In addition, some POA&Ms were significantly beyond their scheduled completion date. Other POA&Ms that were past due were not updated to include a revised completion date nor was a sufficient justification provided as to why they were not closed.

The *National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4* Plan of Action and Milestones CA-5 states:

The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB. Related controls: CA-2, CA-7, CM-4, PM-4.

*Memoranda 02-01 (Guidance for Preparing and Submitting Security Plans of Action and Milestones)* October 17, 2001 states,

Column 1 -- Type of weakness. Describe weaknesses identified by the annual program review, IG independent evaluation or any other work done by or on behalf of the agency.

Column 2 -- Identity of the office or organization that the agency head will hold responsible for resolving the weakness.

Column 3 -- Estimated funding resources required to resolve the weakness. Include the anticipated source of funding, i.e., within the system or as a part of a cross-cutting security infrastructure program. Include whether a reallocation of base resources or a request for new funding is anticipated. This column should also identify other, non-funding, obstacles, and challenges to resolving the weakness, e.g., lack of personnel or expertise, development of a new system to replace insecure legacy system).

Column 4 -- Scheduled completion date for resolving the weakness. Please note that the initial date entered should not be changed. If a weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 9, "Status."

Column 5 -- Key milestones with completion dates. A milestone will identify specific requirements to correct an identified weakness. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the Column 7, "Changes to Milestones."

Column 6 -- Milestone changes. This column would include new completion dates for the milestone.

IAF's current policies and procedures related to POA&Ms were not according to the federal guidance as noted in the criteria above. Also, IAF has not enhanced its process to evaluate the adequacy of justifications provided to extend estimated completion dates to ensure they are met. This includes determining the dependencies and completion of milestones that affect the estimated due date.

POA&Ms are an essential tool to assist management in identifying, prioritizing, and tracking remediation of known security weaknesses. The longer a POA&M item is outstanding, the longer the weakness is exposed which may prevent the control from performing as intended. POA&Ms that are not updated and mitigated in a timely manner cannot be effective at monitoring the progress of corrective efforts related to known weaknesses in IT security controls. As a result, the IAF POA&Ms may not provide an accurate measure of the Foundation's risk related to its information security program effectiveness.

**Recommendation 1:** We recommend IAF's Chief Information Officer develop and implement policies and procedures related to POA&Ms to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to extend estimated completion dates and determine the dependencies and completion of milestones that affect the estimated due dates to ensure that they are met.

## 2. IAF Needs to Periodically Review Policy and Procedures.

**Cybersecurity Framework Security Function:** *All Functions*
**FY20 IG FISMA Metric Domain:** *All Domains*

IAF's policy and procedures were not always periodically reviewed to ensure they address current information security standards. The organization's requirement to review policy and procedure is annually. During our inspection, we found IAF's Information Security Manual, which contains all of its policies was last updated in July 2011. IAF provided an updated Information Security Manual dated July 2020, however, the document is in the draft and not signed. Additionally, the below documents were not reviewed and updated as per IAF's defined frequency:

- IAF Continuity of Operations Plan February 28, 2017;
- IAF Incident Response Plan September 7, 2017; and
- IAF System Security Plan October 1, 2017.

NIST SP 800-53, Revision 4, has 18 controls specifically addressing policies and procedures. The first control of each control family specifies that the organization reviews and updates the current policy and procedures in an Assignment: organization-defined frequency:

a. Reviews and updates the current:
1. Control policy [*Assignment: organization-defined frequency*]; and
2. Control procedures [*Assignment: organization-defined frequency*].

There is no monitoring plan in place to review policies, procedures, and agreements to help ensure compliance with IAF's annual review requirement. Therefore, the CIO may have overlooked reviewing the policies, procedures, and agreements to determine whether they have deviated from current control practices and updating them as needed.

Over time, an agency's security practices may deviate from its written policies and procedures. There is also an increased risk that security practices will become unclear, misunderstood, and improperly implemented.

**Recommendation 2:** We recommend that the IAF's Chief Information Officer create a monitoring plan to review and update policies and procedures in accordance with the timeliness requirements established in agency policies.

## 3. IAF Needs to Update the Continuity of Operations Plan to Include a Business Impact Analysis.

**Cybersecurity Framework Security Function:** *Recover*
**FY19 IG FISMA 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.

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit report.[6] Because that recommendation is still open, we are not making a new recommendation at this time.

[6] Recommendation 2 in *IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-IAF-20-004-C, January 23, 2020).

## 4. IAF Needs to Implement Multi-Factor Authentication for Non-Privileged Accounts.

**Cybersecurity Framework Security Function:** *Protect*
**FY19 IG FISMA 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,* required 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 report.[7] Because that recommendation is still open, we are not making a new recommendation at this time.

[7] Recommendation 7 in *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, IAF outlined its plans to address the two recommendations. IAF's comments are included in their entirety in Appendix IV.

Based on our evaluation of management comments, we acknowledge management decisions on the two recommendations. Further, both recommendations are resolved, but open pending completion of planned activities.

## Appendix I – Scope and Methodology

### Scope

RMA conducted this audit in accordance with GAGAS, as specified in GAO'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 information systems[8] security controls in support of FISMA.

The audit included tests of 86 management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. We assessed IAF's performance and compliance with FISMA in the following areas:

- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information System Continuous Monitoring
- Incident Response
- Contingency Planning

For this audit, we reviewed selected controls related to the FY 2020 IG FISMA Reporting Metrics from five of seven judgmentally selected information systems in IAF's FISMA inventory as of July 2020. See Appendix III for a listing of the 100 control instances that we tested.[9]

The audit also included a follow up on four prior audit recommendations[10,11] to determine if IAF made progress in implementing the recommended improvements concerning its information security program. See Appendix II for status or prior year recommendations.

Audit fieldwork covered IAF's headquarters located in Washington D.C., from April 24, 2020, to September 10, 2020. It covered the period from October 1, 2019, through September 10, 2020.

[8] See Appendix III for a list of the controls and the number of systems selected.

[9] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested 86 controls. A control was counted for each system it was tested against. Thus, there were 100 instances of testing a control. See Appendix III for a list of the controls.

[10] *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).

[11] *IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-IAF-20-004-C, January 23, 2020).

## Methodology

To perform our audit of IAF’s information security program and practices, we followed a work plan based on the OMB and DHS, *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.* We reviewed legal and regulatory requirements stipulated in FISMA and conducted interviews with IAF officials and contractors to determine if IAF implemented an effective information security program. Additionally, we reviewed documentation supporting the information security program. These documents included, but were not limited to, IAF's (1) risk management policy; (2) configuration management procedures; (3) identity and access control measures; (4) security awareness training; and (5) continuous monitoring controls. We compared documentation against requirements stipulated in NIST special publications. Also, we performed tests of information system controls to determine the effectiveness of those controls. Furthermore, we reviewed the status of FISMA audit recommendations for FY 2016 and FY 2019.

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a weakness related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, we tested samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

# Appendix II – Status of Prior Year Findings

The following table provides the status of the FY 2016 and FY 2019 FISMA audit recommendations.[12][13]

*Table 3: FY 2016 & FY 2019 FISMA Audit Recommendations*

| | | Should the recommendation be closed? | |
|---|---|---|---|
| **No.** | **FY 2016 and FY 2019 Audit Recommendations** | **IAF Position** | **Auditor's Position** |
| 1 | Implement multifactor authentication for all network accounts and document the results. | Open | Agree, see finding 4 |
| 2 | 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 Control CM-8, information system component inventory, and IAF's standard operating procedures. | Closed | Agree |
| 3 | Update the Continuity of Operations Plan to include a business impact analysis. | Open | Agree, see finding 3 |
| 4 | 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. | Closed | Agree |

[12] *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).

[13] *IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-IAF-20-004-C January 23, 2020).

## Appendix III – Summary of Controls Reviewed

The following table identifies the controls selected for testing.

*Table 4: Summary of Controls Reviewed*

| No. of Controls in IG Metrics | Control | Control Name | Number of Systems Tested |
|---|---|---|---|
| 1 | AC-1 | Access Control Policy and Procedures | 1 |
| 2 | AC-2 | Account Management | 3 |
| 3 | AC-5 | Separation of Duties | 3 |
| 4 | AC-6 | Least Privilege | 3 |
| 5 | AC-8 | System Use Notification | 1 |
| 6 | AC-11 | Session Lock | 1 |
| 7 | AC-12 | Session Termination | 1 |
| 8 | AC-17 | Remote Access | 1 |
| 9 | AC-19 | Access Control for Mobile Devices | 1 |
| 10 | AU-2 | Audit Events | 1 |
| 11 | AU-3 | Content of Audit Records | 1 |
| 12 | AU-6 | Audit Review, Analysis, And Reporting | 1 |
| 13 | AT-1 | Security Awareness and Training Policy and Procedures | 1 |
| 14 | AT-2 | Security Awareness Training | 1 |
| 15 | AT-3 | Role-Based Security Training | 1 |
| 16 | AT-4 | Security Training Records | 1 |
| 17 | CM-1 | Configuration Management Policy and Procedures | 1 |
| 18 | CM-2 | Baseline Configuration | 1 |
| 19 | CM-3 | Configuration Change Control | 1 |
| 20 | CM-4 | Security Impact Analysis | 1 |
| 21 | CM-6 | Configuration Settings | 1 |
| 22 | CM-7 | Least Functionality | 1 |
| 23 | CM-8 | Information System Component Inventory | 1 |
| 24 | CM-9 | Configuration Management Plan | 1 |
| 25 | CM-10 | Software Usage Restrictions | 1 |
| 26 | CP-1 | Contingency Planning Policy and Procedures | 1 |
| 27 | CP-2 | Contingency Plan | 1 |
| 28 | CP-3 | Contingency Training | 1 |
| 29 | CP-4 | Contingency Plan Testing and Exercises | 1 |
| 30 | CP-6 | Alternate Storage Site | 1 |
| 31 | CP-7 | Alternate Processing Site | 1 |
| 32 | CP-8 | Telecommunications Services | 1 |
| 33 | CP-9 | Information System Backup | 1 |
| 34 | IA-1 | Identification and Authentication Policy and Procedures | 1 |
| 35 | IA-2 | Identification and Authentication (Organizational Users) | 1 |
| 36 | IA-4 | Identifier Management | 1 |
| 37 | IA-5 | Authenticator Management | 1 |
| 38 | IA-7 | Cryptographic Module Authentication | 1 |

| No. of Controls in IG Metrics | Control | Control Name | Number of Systems Tested |
|---|---|---|---|
| 39 | IA-8 | Identification and Authentication (Non-Organizational Users) | 1 |
| 40 | IR-1 | Incident Response Policy and Procedures | 1 |
| 41 | IR-4 | Incident Handling | 1 |
| 42 | IR-6 | Incident Reporting | 1 |
| 43 | IR-7 | Incident Response Assistance | 1 |
| 44 | MP-3 | Media Marking | 1 |
| 45 | MP-6 | Media Sanitization | 1 |
| 46 | PS-1 | Personnel Security Policy and Procedures | 1 |
| 47 | PS-2 | Position Risk Designation | 1 |
| 48 | PS-3 | Personnel Screening | 1 |
| 49 | PS-6 | Access Agreements | 1 |
| 50 | PL-2 | System Security Plan | 1 |
| 51 | PL-4 | Rules of Behavior | 1 |
| 52 | PL-8 | Information Security Architecture | 1 |
| 53 | PM-5 | Information System Inventory | 1 |
| 54 | PM-7 | Enterprise Architecture | 1 |
| 55 | PM-8 | Critical Infrastructure Plan | 1 |
| 56 | PM-9 | Risk Management Strategy | 1 |
| 57 | PM-11 | Mission/Business Process Definition | 1 |
| 58 | RA-1 | Risk Assessment Policy and Procedures | 1 |
| 59 | RA-2 | Security Categorization | 1 |
| 60 | RA-5 | Vulnerability Scanning | 1 |
| 61 | CA-1 | Security Assessment and Authorization Policies and Procedures | 3 |
| 62 | CA-2 | Security Assessments | 1 |
| 63 | CA-3 | System Interconnections | 1 |
| 64 | CA-5 | Plan of Action & Milestones (POA&Ms) | 1 |
| 65 | CA-6 | Security Authorization | 1 |
| 66 | CA-7 | Continuous Monitoring | 1 |
| 67 | SC-7(10) | Boundary Protection\| Prevent Unauthorized Exfiltration | 1 |
| 68 | SC-8 | Transmission Integrity | 1 |
| 69 | SC-10 | Network Disconnect | 1 |
| 70 | SC-13 | Cryptographic Protection | 1 |
| 71 | SC-18 | Mobile Code | 1 |
| 72 | SC-28 | Protection of Information at Rest | 1 |
| 73 | SI-2 | Flaw Remediation | 1 |
| 74 | SI-3 | Malicious Code Protection | 1 |
| 75 | SI-4 | Information System Monitoring | 5 |
| 76 | SI-4(4) | Information System Monitoring\| Inbound and Outbound Communications Traffic | 1 |
| 77 | SI-4(18) | Information System Monitoring\| Analyze Traffic/Cover Exfiltration | 1 |
| 78 | SI-7(8) | Software, Firmware, and Information Integrity\| Auditing Capability for Significant Events | 1 |
| 79 | SA-3 | System Development Life Cycle | 1 |

| No. of Controls in IG Metrics | Control | Control Name | Number of Systems Tested |
|---|---|---|---|
| 80 | SA-4 | Acquisition Process | 1 |
| 81 | SA-8 | Security Engineering Principles | 1 |
| 82 | SA-9 | External Information System Services | 3 |
| 83 | SA-12 | Supply Chain Protection | 1 |
| 84 | SE-2 | Privacy Incident Response | 1 |
| 85 | AR-4 | Privacy Monitoring and Auditing | 1 |
| 86 | AR-5 | Privacy Awareness and Training | 1 |
| **TOTAL CONTROL INSTANCES TESTED** | | | **100** |

## Appendix IV – Management Comments

INTER-AMERICAN FOUNDATION
EMPOWERED COMMUNITIES, SUSTAINABLE RESULTS

**MEMORANDUM**

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

**CC:** Lesley Duncan, COO, Inter-American Foundation

**FROM:** Rajiv Jain Chief Information Officer, /s/

**SUBJECT:** Update, Plan and Action on Recommendations from USAID OIG Audit Report No. A-IAF-21-00X-C dated October 20, 2020

DATE: November 18, 2020

This memorandum provides actions planned and undertaken to address the recommendations contained in the Audit of the Inter-American Foundation's (IAF) Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2020, Draft Audit Report A-IAF- 21-00X-C, dated October 20, 2020.

**Recommendation 1:** Develop and implement policies and procedures related to Plan of Action and Milestones to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to extend estimated completion dates and determine the dependencies and completion of milestones that affect the estimated due dates to ensure that they are met.

IAF agreed with the OIG recommendation and plans on the following corrective actions to complete the mitigation.

a. Document and accurately record relevant information in the POA&M register.
b. Assign criticality to each POA&M.
c. Schedule completion dates.
d. Update new dates for POA&M mitigation and/or accept risk and provide justification for any delays in mitigating POA&M.

Target date: 3/30/2021

**Recommendation 2:** Create a monitoring plan to review and update policies and procedures in accordance with the timeliness requirements established in agency policies.

IAF agreed with the OIG recommendation and plans on the following corrective actions to complete the mitigation.

a. Review and update IAF’s policy and procedures manual at least every two years, to ensure they address current information security standards.
b. Review and update the IAF Continuity of Operations Plan.
c. Review and update the IAF Incident Response Plan.
d. Review and update the IAF System Security Plan.

Target date: 5/30/2021