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

FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended

Audit Report A-IAF-24-002-C
August 23, 2024

Office of Audits, Inspections, and Evaluations

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

MEMORANDUM

DATE: August 23, 2024

TO: Sara Aviel, President and Chief Executive Officer, IAF

FROM Paul K. Martin, Inspector General /s/

SUBJECT: FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended (A-IAF-24-002-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF) information security program for fiscal year (FY) 2024, in support of the Federal Information Security Modernization Act of 2014 (FISMA).[1] 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.[2] To answer the audit objective, RMA assessed the effectiveness of IAF's implementation of the FY 2024 IG FISMA reporting metrics that fall into the nine domains in the following table. [3] Also, RMA assessed IAF's implementation of applicable controls outlined in the National Institute of Standards Technology's Special Publication 800-53, Revision 5,

[1] Pursuant to the Pub. L. No. 117-263 § 5274, USAID OIG provides nongovernmental organizations and/or businesses specifically identified in this report 30 days from the date of report publication to submit a written response to USAID OIG. Any comments received will be posted on https://oig.usaid.gov/. Please direct inquiries to oignotice_ndaa5274@usaid.gov.

[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year IG FISMA reporting metrics.

[3] Office of Management and Budget and Council of the Inspectors General on Integrity and Efficiency's "FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," February 10, 2023.

"Security and Privacy Controls for Information Systems and Organizations," updated December 2020.

RMA reviewed four judgmentally selected systems of the seven in IAF's inventory as of October 16, 2023. RMA's work covered IAF's headquarters in Washington, DC, from September 15, 2023, to May 30, 2024, for the period from October 1, 2023, through May 30, 2024.

RMA concluded that IAF generally implemented an effective information security program. For example, IAF:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured information systems included in its inventory were subject to the monitoring processes defined within IAF's "Information System Continuous Monitoring Strategy."
- Employed automated mechanisms to test system contingency plans.

However, as summarized in the table below, RMA found weakness in three of the nine IG FISMA metric domains. Most significantly, IAF did not remediate serious vulnerabilities within the agency's defined timeframe. These vulnerabilities may be exploited, which can lead to considerable consequences for agency users or systems.

Fiscal Year 2024 **IG FISMA Metric Domains**	**Weaknesses Identified**
Risk Management	
Supply Chain Risk Management	
Configuration Management	X
Identity and Access Management	
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	X
Incident Response	X
Contingency Planning	

RMA also determined that IAF took corrective action on two prior FISMA audit recommendations and that one recommendation remains open.[4] The firm will assess action

[4] IAF took corrective action on recommendation 6 from *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (A-IAF-22-002-C), November 19, 2021. In addition, IAF took corrective action on recommendation 1 while recommendation 3 remains open from *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-IAF-23-001-C), August 28, 2023.

taken to close an additional recommendation from the FY 2023 audit at a later time.[5] Refer to Appendix II of RMA's report for the status of prior year recommendations.

We are making two new recommendations. To address the weaknesses identified in the report, we recommend that IAF's Chief Information Officer take the following actions:

Recommendation 1. Develop and implement a plan, including tools and other resources, to remediate critical and high vulnerabilities within the timeframes specified in the agency's Information System Security Program Standard Operating Procedures (February 2022).

Recommendation 2. Update the agency's system security plan to include controls in National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

In finalizing the report, RMA 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.

[5] Recommendation 2 in *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-IAF-23-001-C), August 28, 2023.

RMA | Associates

Auditors. Consultants. Advisors.

Inter-American Foundation (IAF)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2024

RMA | Associates
Auditors. Consultants. Advisors.

August 23, 2024

Ms. Lisa Banks
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 Ms. Banks:

The independent certified public accounting firm, RMA Associates, LLC, is pleased to present our report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024.

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

Thank you,

Reza Mahbod

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

RMA | Associates
Auditors. Consultants. Advisors.

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

August 23, 2024

RMA Associates, LLC, 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 scope of this audit was to assess IAF's information security program, which is consistent with FISMA, and reporting instructions issued by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. The audit included tests of applicable controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated December 2020.

For this audit, we reviewed four of seven judgmentally selected systems in IAF's inventory as of October 16, 2023. Our work covered IAF's headquarters located in Washington, D.C., from September 15, 2023, to May 30, 2024.

Our audit was performed 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We concluded that IAF implemented an effective information security program. However, we found weaknesses in IAF's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in three Inspector General FISMA Metric Domains primarily due to IAF not adhering to its policies and procedures in accordance with the National Institute of Standards and Technology Special Publication 800, Revision 5. We made two recommendations to assist IAF in strengthening its information security program.

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

Respectfully,

RMA Associates

RMA Associates LLC

Table of Contents

Summary of Results 1
Background 1
Audit Results 2

Audit Findings 4
1. IAF Needs to Remediate Critical and High Vulnerabilities Within Its Defined Remediation Timeframe. 4
2. IAF Authorized a System to Operate Without Including the Required NIST SP 800-53 Revision 5 Controls in the Control Assessment. 5
3. IAF Needs to Implement Event Logging Requirements Set Forth by OMB M-21-31. 6

Evaluation of Management Comments 8

Appendix I – Scope and Methodology 9
Scope 9
Methodology 10

Appendix II - Status of Prior Year Recommendations 11

Appendix III – Management Comments 13

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 evaluation of the Inter-American Foundation's (IAF) information security program for fiscal year (FY) 2024. The audit objective of this performance audit was to determine whether IAF implemented an effective information security program.[2]

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.

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.

FISMA also requires the agency inspectors general (IGs) to assess the effectiveness of agency information security programs and practices and report the results of the assessments to the Office of Management (OMB). Annually, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) provide instructions to Federal agencies and IGs for assessing agency information security programs.

The FY 2024 metrics are designed to assess the maturity[3] of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the 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 was defined as having an overall mature program based on the current year Inspector General FISMA reporting metrics.

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

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2024 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain 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

Audit Results

This audit was performed in accordance with generally accepted government auditing standards. RMA determined that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objective.

The audit concluded that IAF generally implemented an effective information security program. For example, IAF:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured information systems included in its inventory were subject to the monitoring processes defined within IAF's *Information System Continuous Monitoring Strategy*.
- Employed automated mechanisms to test system contingency plans.

As shown in Table 2, the overall maturity of IAF's information security program was Managed and Measurable (Effective).

Table 2: FY 2024 IAF Maturity Level

Cybersecurity Framework Security Functions	Core Metric	FY 24 Supplemental Metric	FY 24 Assessed Maturity Level
Identify	Effective	Effective	Managed and Measurable
Protect	Effective	Effective	Managed and Measurable
Detect	Ineffective	Effective	Managed and Measurable
Respond	Effective	Effective	Managed and Measurable
Recover	Effective	Effective	Managed and Measurable
Overall	Effective	Effective	**Managed and Measurable**

However, we found weaknesses in IAF's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. As a result, we noted weaknesses in three IG FISMA Metric Domains (Table 3) and presented recommendations to strengthen the agency's information security program.

Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2024 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Identify	Risk Management	None
	Supply Chain Risk Management	None
Protect	Configuration Management	IAF Needs to Remediate Critical and High Vulnerabilities Within Its Defined Remediation Timeframe (Finding 1).
	Identity and Access Management	None
	Data Protection and Privacy	None
	Security Training	None
Detect	Information Security Continuous Monitoring	IAF Authorized a System to Operate Without Including the Required NIST SP 800-53 Revision 5 Controls in the Control Assessment (Finding 2).
Respond	Incident Response	IAF Needs to Implement Event Logging Requirements Set Forth by OMB M-21-31 (Finding 3).
Recover	Contingency Planning	None

We are making two new recommendations to address the weaknesses. In addition, as shown in Appendix II, IAF has not yet taken final corrective action on one of four prior FISMA audit recommendations, and we will review IAF's corrective actions taken for another recommendation at a later time. Detailed findings appear in the following section.

Audit Findings

1. IAF Needs to Remediate Critical and High Vulnerabilities Within Its Defined Remediation Timeframe.

Cybersecurity Framework Security Function: *Protect*
FY24 IG FISMA Metric Domain: *Configuration Management*

IAF did not remediate its vulnerabilities within the IAF-defined timeframe. We identified 181 critical vulnerabilities and 623 high vulnerabilities[4] that were not remediated in accordance with the timeframes outlined in IAF's standard operating procedures. By the end of the audit fieldwork, the critical and high vulnerabilities had exceeded IAF's remediation timeframes by 100-200 days.

NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations states:

> **SI-2 FLAW REMEDIATION**
>
> Control: The organization identifies, reports, and corrects information system flaws
>
> **RA-5 VULNERABILITY MONITORING AND SCANNING**
>
> Control: The organization remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk

In addition, IAF's *Information System Security Program Standard Operating Procedures* (February 2022) states:

> IAF Office of Operation teams (e.g., Network Administrators, System administrators) are responsible for coordinating remediation of legitimate vulnerabilities based on the following risk priority schedule and timeframes in accordance with Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 19-02, "Vulnerability Remediation Requirements for Internet-Accessible Systems:"
>
> - Critical: 15-day remediation
> - High Vulnerabilities: 30-day remediation

According to IAF officials, the agency was not efficient in its efforts to remediate critical and high vulnerabilities due to its limited resources and new security tools. IAF officials stated that a new scan showed some vulnerabilities were resolved based on progress made through the implementation of automation. For the remaining vulnerabilities, IAF personnel were in the process of receiving and applying new patches or uninstalling certain software. Nonetheless, IAF

[4] Critical vulnerabilities are the most severe security weaknesses in software, hardware, or systems. These vulnerabilities are highly exploitable, can lead to severe consequences, and affect large number of users or systems. High vulnerabilities are also severe but slightly less critical. They usually are likely to be exploited, can lead to significant consequences, and affect many users or systems.

officials acknowledged that they did not have a plan to assure critical and high vulnerabilities would be given the highest priority so they would be remediated within agency timeframes.

Unmitigated vulnerabilities can compromise the confidentiality, integrity, and availability of information. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Authorized users may not be able to access the system.
- Agency data may be lost, stolen, or compromised.

Recommendation 1: *We recommend that IAF's Chief Information Officer develop and implement a plan, including tools and other resources, to remediate critical and high vulnerabilities within the timeframes specified in the agency's* Information System Security Program Standard Operating Procedures (February 2022).

2. IAF Authorized a System to Operate Without Including the Required NIST SP 800-53 Revision 5 Controls in the Control Assessment.

Cybersecurity Framework Security Function: *Detect*
FY24 IG FISMA Metric Domain: *Information Security Continuous Monitoring*

IAF's system security plan (SSP) for one system (January 2021) states:

> **PL-02 SYSTEM SECURITY PLAN**
> Control: The organization:
> - Reviews the security plan for the information system annually;
> - Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
> - Protects the security plan from unauthorized disclosure and modification.

In addition, IAF's *Information System Security Program Standard Operating Procedures* states that "all controls must be assessed during the authorization process."

IAF did not update its SSP for one of four systems reviewed to include new controls before completing the system's authorization to operate package for review and approval. Specifically, the SSP did not include the new controls required controls by NIST SP 800-53, Revision 5. Instead, IAF partially updated the SSP but accepted the risk of omitting the new NIST SP 800-53, Revision 5, controls because, according to the Security Assessment Report, the risk associated with the omitted controls was low.

As a result of the omitted controls, IAF officials authorized the system to operate without assuring all controls necessary to protect it were implemented. Because IAF categorized the system as moderate impact, meaning loss of confidentiality, integrity, or availability is expected to have a serious adverse effect, we are making the following recommendation.

Recommendation 2: *We recommend that IAF's Chief Information Officer update its system security plan to include National Institute of Standards and Technology Special Publication 800-53, Revision 5, controls.*

3. IAF Needs to Implement Event Logging Requirements Set Forth by OMB M-21-31.

Cybersecurity Framework Security Function: *Respond*
FY24 IG FISMA Metric Domain: *Incident Response*

IAF did not meet the Event Logging (EL) requirements at maturity EL2 (intermediate) and EL3 (advanced) levels, in accordance with OMB memorandum M-21-31. As of April 25, 2024, or 30 months since issuance, IAF had not met either EL2 or EL3. Instead, IAF was at maturity EL1 (basic) level. However, IAF was required to reach EL2 maturity within 18 months of the memorandum, which was issued on August 27, 2021. Furthermore, the memorandum set forth the deadline of August 2023 for adherence to EL3 (advanced) requirements.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, states:

> Section I: Maturity Model for Event Log Management
>
> Tier EL3, Rating – Advanced
>
> The agency and all its components meet the following requirements, as detailed in Table 4 (EL3 Advanced Requirements) within Appendix A (Implementation and Centralized Access Requirements):
>
> - Meeting EL2 maturity level
> - Advanced Logging Categories
> - Logging Orchestration, Automation, and Response – Finalizing Implementation
> - User Behavior Monitoring – Finalizing Implementation
> - Application Container Security, Operations, and Management
> - Advanced Centralized Access
>
> Section II: Agency Implementation Requirements
>
> Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
>
> - Within one year of the date of this memorandum, reach EL1 maturity.
> - Within 18 months of the date of this memorandum, achieve EL2 maturity.
> - Within two years of the date of this memorandum, achieve EL3 maturity.

According to IAF officials, IAF did not meet the logging requirements at the EL3 (advanced) maturity level due to the high cost. They explained that they have requested funding to meet both EL2 and EL3 logging requirements and will not achieve these levels until the funding is received. IAF management stated that they have identified an EL3 logging solution and are awaiting funding approval.

By not meeting the logging requirements at maturity EL3 (advanced), IAF decreases its ability to ensure the highest-level security operations center and accelerate incident response efforts to enable more effective defense of Federal information.

A recommendation addressing EL2 was made in the FY 2023 FISMA audit report.[5] In IAF's revised management decision in response to that recommendation, IAF officials planned to take action that will address EL2 and EL3 requirements. Therefore, we are not making a recommendation to address this weakness at this time.

[5] Recommendation 3 in *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report A-IAF-23-001-C, August 28, 2023).

Evaluation of Management Comments

In response to the draft report, IAF outlined its plan to address recommendations 1 and 2. IAF’s comments are included in their entirety in Appendix III. Based on our evaluation of management comments, we acknowledge management’s decision on recommendations 1 and 2. Further, the recommendations are open pending the completion of planned activities.

Appendix I – Scope and Methodology

Scope

RMA 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit tested the core and supplemental metrics for FY 2024 identified in the *FY 2023-2024 IG FISMA Reporting Metrics* issued by OMB and the CIGIE.

The scope of this audit was to assess whether IAF's information security program was consistent with FISMA, and the reporting instructions issued by OMB and the CIGIE. In addition, the audit included tests of applicable controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, updated December 2020. We assessed IAF's performance and compliance with FISMA in the following control areas:

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

We conducted a risk assessment to identify a representative number of systems (a minimum of two internal and two external) to be tested when needed for system-level testing. Only moderate systems not previously tested in the prior year. Four out of seven internal and external systems were selected for FY 2024 in IAF's current system inventory as of October 4, 2023, to meet the requirement.

The audit also included a follow-up on four prior audit recommendations[6,7] to determine if IAF implemented the recommended improvements concerning its information security program. See Appendix II for the status of those recommendations.

Our work was conducted at IAF's headquarters located in Washington, DC, from September 15, 2023, to May 30, 2024. It covered the period from October 1, 2023, through May 30, 2024.

[6] Recommendation 6, *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report A-IAF-22-002-C, November 19, 2021).

[7] Recommendations 1-3, *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report A-IAF-23-001-C, August 28, 2023).

Methodology

To determine if IAF implemented an effective information security program, RMA conducted interviews with IAF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, RMA 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. RMA compared documentation against requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls, including a vulnerability assessment, to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of four FISMA audit recommendations for FY 2023 and FY 2021.

In testing the effectiveness of the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them. RMA 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 deficiency 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, RMA 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 Recommendations

The following table provides the status of the FY 2023 and FY 2021 FISMA audit recommendations.[8,9]

Table 4: FY 2023 & 2021 FISMA Audit Recommendations

Audit Report & Recommendation No.	Audit Recommendations	IAF's Corrective Action Plan	IAF's Position	Auditor's Position on the Status
A-IAF-23-001-C (Rec.1)	We recommend that IAF's Chief Information Officer improve the record keeping process to maintain records of the first day its users access agency systems.	IAF is using an AT&T USM Anywhere Subscription that maintains audit records for the life of the service at a minimum of 1 year in accordance with IAF's security policy.	Closed	Agree, but pending official closure notification
A-IAF-23-001-C (Rec.2)	We recommend that IAF's Chief Information Officer develop and implement procedures for compensating controls in lieu of multifactor authentication (MFA) for systems that the agency plans to decommission.	IAF accepted the MFA risk for the remainder of the WebGrants application life. As of April 30, 2024, the WebGrants application was decommissioned and is no longer in use.	Closed	Pending review

[8] *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report A-IAF-22-002-C, November 19, 2021).

[9] *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report A-IAF-23-001-C, August 28, 2023).

Audit Report & Recommendation No.	Audit Recommendations	IAF's Corrective Action Plan	IAF's Position	Auditor's Position on the Status
A-IAF-23-001-C (Rec.3)	We recommend that IAF's Chief Information Officer implements level 2 event logging requirements in accordance with Office of Management and Budget Memorandum, M-21-31.	IAF plans on doing the following corrective actions to complete the mitigation: 1. Research solutions to implement Event Logging (EL) tier 3 in accordance with OMB M-21-31. 2. Allocation of funding for an EL3 tier logging solution. 3. Implement the audit solution for compliance with Event Logging tier 3. 4. IAF will continue at EL1 and accept the risk until an affordable EL3 logging solution is available.	Open	Open
A-IAF-22-002-C (Rec.6)	We recommend that IAF's Chief Information Officer document and implement a written process for obtaining and evaluating feedback on IAF's privacy and security training content, including role-based training.	IAF developed a training evaluation form to be used by the Chief Information Security Officer to collect feedback on various agency training content. Also, IAF updated the IAF Information System Security Program Standard Operating Procedures to include a new training feedback process for obtaining and evaluating feedback on security, privacy, and role-based training.	Closed	Agree, but pending official closure notification

Appendix III – Management Comments

INTER-AMERICAN FOUNDATION
EMPOWERED COMMUNITIES, SUSTAINABLE RESULTS

MEMORANDUM

TO: IG/A/ITA, Lisa Banks, Director, USAID OIG

FROM: Duleep Sahi, Chief Information Officer /s/

Cc: Lesley Duncan, Chief Operating Officer

DATE: July 31, 2024

SUBJECT: Inter-American Foundation (IAF) Comments, Plan and Action on Recommendations from USAID OIG Draft Audit Report No. A-IAF-24-00X-C dated July 24, 2024.

This memorandum provides Inter-American Foundation (IAF)'s management comments and 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 2024, Audit Report A-IAF-24-00X-C, dated July 24, 2024.

The scope of this audit was to evaluate the IAF's information security program for fiscal year (FY) 2024 in accordance with FISMA requirements. The audit objective of this performance audit was to determine whether IAF implemented an effective information security program.
The FY 2024 metrics are designed to assess the maturity of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover.

The IAF is pleased that the auditors found that overall the Agency's information security program was calculated as Managed and Measurable (Effective) while noting weaknesses in three of the nine Inspector General FISMA Metric Domains. The IAF accepts the determination of the auditors and appreciates the engagement opportunity.

Recommendation 1. Develop and implement a plan, including tools and other resources, to remediate critical and high vulnerabilities within the timeframes specified in the IAF Information System Security Program Standard Operating Procedures.

IAF agrees with the OIG recommendation and will develop a vulnerability remediation strategy and plan, including tools and resources, to remediate critical and high vulnerabilities within agency established timeframes.

Target date: 12/31/2024

Recommendation 2. Update the Enterprise Network system security plan to include controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

IAF agrees with the OIG recommendation and will update the Enterprise Network system security plan with the NIST SP 800-53, Revision 5, security and privacy controls for the system.

Target date: 02/28/2025

In response to the open prior year recommendation (**A-IAF-23-001-C (Rec.3**)) regarding implementing event logging requirements set forth by OMB M-21-31, the IAF has identified a solution and requested funding through the agency budget process.

Target date: 04/01/2026

There is no information in the draft report that the agency believes should be withheld from public release under the Freedom of Information Act. If you have any questions or require additional information, please contact me at 202-688-6107 or dsahi@iaf.gov.