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

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

Information Technology Audits Division

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

MEMORANDUM

DATE: August 28, 2023

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

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

SUBJECT: IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA (A-IAF-23-001-C)

Enclosed is the final audit report on the Inter-American Foundation (IAF) information security program for fiscal year 2023, 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 2023 IG FISMA reporting metrics[3] that fall into the nine domains in

[1] Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 5274, which amends the Inspector General Act of 1978, when USAID OIG contracts with an audit firm to perform the work, USAID OIG provides non-governmental organizations and/or business entities specifically identified in the accompanying report, if any, 30 days from the date of report publication to review the final report and submit a written response to USAID OIG that clarifies or provides additional context for each instance within the report in which the non-governmental organization and/or business entity is specifically identified. Any comments received to this effect are posted for public viewing on https://usaid.oig.gov with USAID OIG's final transmittal. Please direct related inquiries to oignotice_ndaa5274@usaid.gov.

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

the following table. Also, RMA assessed IAF's implementation of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

RMA reviewed four of six judgmentally selected systems in IAF's inventory as of October 19, 2022. Audit fieldwork covered IAF's headquarters located in Washington, DC, from September 15, 2022, to June 14, 2023, for the period from October 1, 2022, through June 14, 2023.

RMA concluded that IAF generally implemented an effective information security program, considering the unique mission, resources, and challenges of the agency. 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, and
- Employed automated mechanisms to test system contingency plans.

However, as summarized in the table below, RMA found weaknesses in two of the nine FY 2023 IG FISMA metric domains.

Fiscal Year 2023 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	
Supply Chain Risk Management	
Configuration Management	
Identity and Access Management	X
Data Protection and Privacy	
Security Training	
Information Security Continuous Monitoring	
Incident Response	X
Contingency Planning	

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

Recommendation 1. Improve the record keeping process to maintain records of the first day its users access agency systems.

Recommendation 2. Develop and implement procedures for compensating controls in lieu of multifactor authentication for systems that the agency plans to decommission.

Recommendation 3. Implement level 2 event logging requirements in accordance with Office of Management and Budget Memorandum, M-21-31.

In finalizing the report, RMA evaluated IAF's responses to the recommendations. After reviewing that evaluation, we consider recommendation 1 resolved but open pending OIG's verification of IAF's final actions, and recommendations 2 and 3 resolved but open pending completion of planned activities. For recommendations 2 and 3, please provide evidence of final action to OIGAuditTracking@usaid.gov.

In addition, IAF took final corrective action on seven of eight open recommendations from the FY2020[4] and FY2021[5] FISMA audits. Refer to Appendix II on page 10 of RMA's report for the status of prior year recommendations.

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

[4] Recommendation 2 in *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-IAF-21-002-C, December 4, 2020).

[5] Recommendations 1, 2, 3, 6, 7, 8, and 9 in *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).

RMA | Associates
Auditors. Consultants. Advisors.

Inter-American Foundation (IAF)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2023

RMA | Associates
Auditors. Consultants. Advisors.

August 24, 2023

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:

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 2023.

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.

Respectfully,

Reza Mahbod

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.

August 24, 2023

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 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 management, technical, and operational 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 September of 2020.

For this audit, we reviewed four of six judgmentally selected systems in IAF's inventory as of October 19, 2022. Audit fieldwork covered IAF's headquarters located in Washington, DC, from September 15, 2022, to June 14, 2023.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards, as specified in 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.

We concluded that IAF generally implemented an effective information security program based on IAF's overall implementation of security controls and considering the unique mission, resources, and challenges of IAF. 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 two of the nine Inspector General FISMA Metric Domains. We made three 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
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 audit of the Inter-American Foundation's (IAF) information security program for fiscal year (FY) 2023. The 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).

The FY 2023 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) 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 having an overall mature program based on the current year Inspector General FISMA reporting metrics.

[3] 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.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2023 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2023 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

This audit was performed in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. RMA determined the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

The audit concluded that IAF generally implemented an effective information security program, considering the unique mission, resources, and challenges of the agency. 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; and
- 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 2023 IAF Maturity Level

Cybersecurity Framework Security Functions	FY 23 Assessed Maturity Level	Effective?
Identify	Managed and Measurable	Yes
Protect	Consistently Implemented	Yes[4]
Detect	Managed and Measurable	Yes
Respond	Managed and Measurable	Yes
Recover	Managed and Measurable	Yes
Overall	**Managed and Measurable**	Yes

[4] Although the audit determined that IAF's Protect function was Consistently Implemented, this is effective considering IAF's unique mission, resources, and challenges.

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 two 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 2023 FISMA Assessment

Cybersecurity Framework Security Functions	**FY 2023 IG FISMA Metric Domains**	**Weakness Noted in FY 2023**
Identify	Risk Management	None
Identify	Supply Chain Risk Management	None
Protect	Configuration Management	None
Protect	Identity and Access Management	IAF Could Not Assess Whether its New Users Completed Access Forms Before Accessing Its Systems (Finding 1). IAF Did Not Fully Implement Multifactor Authentication (Finding 2).
Protect	Data Protection and Privacy	None
Protect	Security Training	None
Detect	Information Security Continuous Monitoring	None
Respond	Incident Response	IAF Did Not Implement Level 2 Event Logging Requirements (Finding 3).
Recover	Contingency Planning	None

We are making three new recommendations to address the weaknesses identified. In addition, as illustrated in Appendix II, we agree that IAF has taken final corrective action on seven prior FISMA audit recommendations. We will evaluate the remaining recommendation at a later time. Detailed findings appear in the following section.

Audit Findings

1. IAF Could Not Assess Whether its New Users Completed Access Forms Before Accessing Its Systems.

Cybersecurity Framework Security Function: *Protect*
FY23 IG FISMA Metric Domain: *Identity and Access Management*

IAF could not determine whether its new users signed access agreements prior to being granted access to its systems. Specifically, from a universe of three users, IAF could not confirm whether two completed the forms before they accessed the system.

NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, states:

> **PS-6 ACCESS AGREEMENTS**
>
> Control:
> c. Verify that individuals requiring access to organizational information and systems:
> 1. Sign appropriate access agreements prior to being granted access;

According to IAF officials, due to issues with migrating to a new system, IAF did not maintain records of the first day users accessed the system. Even though IAF had a process to maintain records, that process needed to be enhanced to maintain records of the first day its users accessed the agency's system.

As a result, IAF did not have assurance that its users had a clear understanding of their rights, responsibilities, and limitations when accessing and using the information system. Further, users may not be aware of their responsibilities in maintaining security, resulting in increased risks to the system's integrity and confidentiality. Moreover, IAF was at risk that users may leave the system vulnerable to security breaches, unauthorized access, and misuse.

Recommendation 1: *We recommend that IAF's Chief Information Officer improve its current record keeping process to maintain records of the first day its users access the agency's systems.*

2. IAF Did Not Fully Implement Multifactor Authentication.

Cybersecurity Framework Security Function: *Protect*
FY23 IG FISMA Metric Domain: *Identity and Access Management*

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

IA-2 IDENTIFICATION AND AUTHENTICATION (Organizational Users)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: 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.

Control Enhancements:

2. Implement multi-factor authentication for access to non-privileged accounts

IAF did not implement multifactor authentication in one of the four selected systems. According to IAF officials, the system was scheduled to be decommissioned in Fall 2023. As such, IAF did not implemented multifactor authentication. However, IAF did not implement compensating controls until the time the system will be decommissioned. Further, IAF did not have procedures to assure such controls would be in place. By not fully implementing multifactor authentication, IAF increased the risk of unauthorized individuals gaining access to its information system and data.

Recommendation 2: *We recommend that IAF's Chief Information Officer develop and implement procedures for compensating controls in lieu of multifactor authentication for systems that the agency plans to decommission.*

3. IAF Did Not Implement Level 2 Event Logging Requirements.

Cybersecurity Framework Security Function: *Respond*
FY23 IG FISMA Metric Domain: *Incident Response*

IAF was required to reach Event Logging level 2 (EL2), intermediate, within 18 months of OMB M-21-31, which was issued August 27, 2021. However, as of May 2, 2023—21 months after issuance of the memorandum—IAF did not meet the EL2 requirements and was still at Event Logging level 1 (EL1), basic. For example, IAF's event logs did not capture the date, time, source, and destination of cyber incidents as well as monitor network bandwidth usage.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, states that to meet EL2, agencies must meet the following requirements:

- Meeting EL1 maturity level
- Intermediate Logging Categories [See Appendix III of this report for details]
- Publication of Standardized Log Structure
- Inspection of Encrypted Data

...

> 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.
>
> …
>
> The Retention Period required the utilization of the 12 Months Active Storage and 18 Months Cold Data Storage.

According to IAF officials, IAF did not meet EL2 logging requirements due to the complexity and volume of logging requirements. In addition, IAF officials said that, due to limited resources and competing priorities, IAF did not employ sufficient resources to fully comply with OMB M-21-31.

By not meeting EL2 (intermediate) logging requirements, IAF may not be able to accelerate incident response efforts to enable more effective defense of the agency's information.

Recommendation 3: *We recommend that IAF's Chief Information Officer implement level 2 event logging requirements in accordance with M-21-31.*

Evaluation of Management Comments

In response to the draft report, IAF outlined its plans to address the three recommendations. IAF's comments are included in their entirety in Appendix IV.

Based on our evaluation of management comments, we acknowledge IAF's management decisions on all three recommendations. Further, we consider recommendation 1 resolved but open pending OIG's verification of the Agency's final actions, and recommendations 2 and 3 resolved but open pending completion of planned activities.

Appendix I – Scope and Methodology

Scope

RMA conducted this performance audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit was conducted for Fiscal Year (FY) 2023 and tested the core and supplemental metrics identified in the *FY 2023-2024 Inspector General (IG) Federal Information Modernization Act of 2014 (FISMA) Reporting Metrics* issued by OMB and the Council of the Inspectors General on Integrity and Efficiency.

The scope of this audit was to assess IAF's information security program 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. In addition, the audit included tests of management, technical, and operational controls outlined in National Institute Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.* 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 System Continuous Monitoring
- Incident Response
- Contingency Planning

For this audit, we reviewed four of six judgmentally selected systems in IAF's inventory as of October 19, 2022. The audit also included a follow-up on seven prior audit recommendations[5][6] to determine if IAF made progress in implementing them. See Appendix II.

Audit fieldwork was conducted at IAF's headquarters located in Washington, DC, from September 15, 2022, to June 14, 2023. It covered the period from October 1, 2022, through June 14, 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

[5] Recommendation 2 in *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-IAF-21-002-C December 4, 2020).

[6] Recommendations 1-3 and 7-9 in *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).

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 FISMA audit recommendations for FY 2020 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 Fiscal Year (FY) 2021 and FY 2020 FISMA audit recommendations.[7][8]

Table 4: FY 2021 & 2020 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2023 Audit Recommendations	IAF's Position	Auditor's Position on the Status
A-IAF-22-002-C (Rec.1)	Fully document and implement a process to include in the risk acceptance forms a clear business reason for risk acceptance and the compensating controls implemented to reduce the risk that vulnerabilities can be exploited.	Closed	Agree
A-IAF-22-002-C (Rec.2)	Develop and implement supply chain risk management policies, procedures, and strategies	Closed	Agree
A-IAF-22-002-C (Rec.3)	Develop and implement a procedure to document risk acceptance when vulnerabilities cannot be remediated within the timeframes specified in IAF's operating procedures.	Closed	Agree
A-IAF-22-002-C (Rec.6)	Document and implement a written process for obtaining and evaluating feedback on IAF's privacy and security training content, including role-based training.	Closed	Will be assessed later.
A-IAF-22-002-C (Rec.7)	Develop and implement a process to document lessons learned related to risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring to improve IAF's security posture.	Closed	Agree
A-IAF-22-002-C (Rec.8)	Develop and implement an information security continuous monitoring strategy.	Closed	Agree
A-IAF-22-002-C (Rec.9)	Develop and implement a written process to document participants in IAF's contingency plan training.	Closed	Agree
A-IAF-21-002-C (Rec.2)	Create a monitoring plan to review and update policies and procedures in accordance with the timeliness requirements established in agency policies.	Closed	Agree

[7] *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)

[8] *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-IAF-21-002-C December 4, 2020).

Appendix III – OMB M-21-31 Event Log Level 2 Requirements

According to OMB-M-21-31, agencies must implement the following Event Log Level 2 requirements:

- Network Device Infrastructure (for Devices with Multiple Interfaces: Interface Media Access Control (MAC) - If Correlated to the De-NAT Internet Protocol (IP) Address) - All Devices: IDs / IPs Alerts and Events
  - Date and Time
  - Source
    - Hostname
    - IP Address and Port
    - MAC
  - Destination
    - Hostname
    - IP Address and Port
    - MAC
  - Signature Triggered and Associated Details Including:
    - Signature
    - Anomaly
  - Rate Threshold
  - Device Name
  - Type of Event and Category
  - In the Case of Fortinet Network IPs, Attack Context
  - (Web / Device) User Agent if Available
  - Wi-Fi Channel
  - Wi-Fi Extended Service Set Identifier (ESSID)
- Application Level - Web Applications
  - Uniform Resource Locator (URL)
  - Headers
  - Hypertext Transfer Protocol (HTTP) Methods - Request with Body of Data14
  - HTTP Response with Body of Data
- Network Traffic - Full Packet Capture Data
  - Decrypted Plaintext
  - Cleartext
- Application Level - General – Non- Commercial Off the Shelf (COTS)
  - User Authentication (Success/Failure)
  - User Access of Application Components
    - File and Object Access
    - Audit Log Access (Success/Failure)
    - System Access (Failure)
    - Application Transactions
  - Transaction Logs
  - System Performance and Operational Characteristics
    - Resource Utilization

    - Errors (Input Validation, Dis-allowed Operations)
    - Process Status
    - Service Status Changes (e.g., Started, Stopped)
  - Application Configuration and Version, Middleware Configuration and Version
  - Usage Information, if Applicable
  - User Request and Response Events, if Applicable

Appendix IV – 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: August 10, 2023

SUBJECT: Inter-American Foundation (IAF) Comments, Plan and Action on Recommendations from USAID OIG Draft Audit Report No. A-IAF-23-00X-C dated July 31, 2023.

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 2023, Audit Report A-IAF- 23-00X-C, dated July 31, 2023.

The scope of this audit was to evaluate the IAF's information security program for fiscal year (FY) 2023 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 2023 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 auditors noted weaknesses in two of the nine Inspector General FISMA Metric Domains. Overall, the IAF's information security program was calculated as Managed and Measurable (Effective).

The IAF accepts the determination of the auditors and appreciates the engagement opportunity. 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.

Recommendation 1. Improve its record keeping process to maintain records of the first day its users access agency systems.

In response to Recommendation 1, IAF has performed the following action items and consequently final action has been taken on the recommendation:

a. IAF procured a new audit record subscription service from AT&T that maintains audit records for the life of the service and at a minimum – for 1 year in accordance with IAF security policy.
b. AT&T by default backs up IAF audit records automatically into a secure cloud environment.

Completed date: 08/01/2023
Supplementary document/evidence attached:

IAF AT&T USM Anywhere Subscription Service Contract
USM Anywhere data security link with retention information:
https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/admin/usm-anywhere-data-security.htm

Recommendation 2. Develop and implement procedures for compensating controls in lieu of multifactor authentication for systems that the agency plans to decommission.

IAF agrees that the WebGrants application is out of compliance with multifactor authentication, however, the new GovGrants application (to be online as of October 1, 2023) will have multifactor authentication. IAF will accept the risk for the remaining one and a half months of WebGrants application life.

Target date: 10/31/2023

Recommendation 3. Implement level 2 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31.

IAF agrees with the OIG recommendation and plans on the following corrective actions to complete the mitigation:

a. Research solutions to implement Event Logging (EL) tier 3 in accordance with OMB M-21-31.
b. Allocation of funding for an EL3 tier logging solution.
c. Implement the audit solution for compliance with Event Logging tier 3.
d. IAF will continue at EL1 and accept the risk until at such time an affordable EL3 logging solution is made available.

Target date: 04/01/2024