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

IAF Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA

Audit Report A-IAF-22-007-C
September 2, 2022

Information Technology Audits Division

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

MEMORANDUM

DATE: September 2, 2022

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

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

SUBJECT: IAF Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA (A-IAF-22-007-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF) information security program for fiscal year 2022, 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 the maturity level IAF achieved for each of its core FISMA reporting metrics.[1] Therefore, it was not designed to determine causes of, effects of, or make recommendations to improve the maturity levels.

To answer the audit objective, RMA assessed the maturity level of IAF's implementation of the 20 core metrics. The scope of this audit was to assess whether IAF's information security program was consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security.[2] Also, RMA assessed IAF's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. RMA reviewed 4 of 6 judgmentally selected information systems in IAF's

[1] For this audit, "core metrics" are defined as the FY 2022 inspector general FISMA reporting metrics issued by the Office of Management and Budget, Office of the Federal Chief Information Officer, "FY22 Core IG Metrics Implementation Analysis and Guidelines," April 13, 2022.
[2] "FY 2022 Core IG FISMA Metrics Evaluation Guide"

inventory as of February 14, 2022. Audit fieldwork covered IAF's headquarters in Washington, DC. Fieldwork was performed from March 23, 2022, through July 7, 2022, and covered the period from October 1, 2021, through July 7, 2022.

RMA concluded that, for the 20 core metrics, IAF's information security program was managed and measurable for 9 metrics, consistently implemented for 5 metrics, and defined for 6 metrics. Therefore, IAF's information security program was calculated as managed and measurable.

In finalizing the report, the audit firm received IAF's concurrence with the assessed maturity levels for the 20 core metrics. Although the audit report did not contain recommendations, IAF management said they will review the metrics assessed at the defined maturity level for possible remediation.

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

RMA | Associates

Auditors. Consultants. Advisors.

Inter-American Foundation (IAF)

Federal Information Security Modernization Act of 2014
(FISMA)

Final Report
Fiscal Year 2022

RMA | Associates

Auditors. Consultants. Advisors.

September 2, 2022
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 final report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022.

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

Table of Contents

RMA | Associates
Auditors. Consultants. Advisors.

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

September 2, 2022

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 what maturity level IAF achieved for each of its core FISMA reporting metrics. The scope of this audit was to assess whether IAF's information security program was consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit included tests of management, technical, and operational controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated December 10, 2020.

For this audit, we reviewed four of six judgmentally selected systems in IAF's inventory as of February 14, 2022. Audit fieldwork covered IAF's headquarters located in Washington, D.C., from March 23, 2022, to July 7, 2022.

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 concluded that, for the 20 core metrics, IAF's information security program was Defined for 6 metrics, Consistently Implemented for 5 metrics, and Managed and Measurable for 9 metrics.

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

Summary of Results

Background

The United States Agency for International Development's Office of Inspector General 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) 2022. The objective of this performance audit was to answer the following question:

> What maturity level did IAF achieve for each of its core FISMA reporting metrics?[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 their agency’s information security programs and practices and report the results of the assessments to the Office of Management (OMB).

Annually, OMB and the Department of Homeland Security provide instructions to Federal agencies and IGs for assessing agency information security programs. On December 6, 2021, OMB issued OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements.* According to that memorandum, each year, IGs are required to complete metrics[3] to independently assess their agencies' information security programs.

The FY 2022 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 4.0: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1. Table 2 defines each maturity level.

[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 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, “core metrics” are defined as the FY 2022 inspector general FISMA reporting metrics.

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

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2022 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2022 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

Table 2: Maturity Level Definitions

Maturity Level	Maturity Level Description *
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner. Achieving this maturity level is not effective.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented. Achieving this maturity level is not effective.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. Achieving this maturity level is not effective.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes. Achieving this maturity level is effective.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs. Achieving this maturity level is effective.

* FY 2022 Core IG FISMA Metrics define which maturity levels are considered to be effective.

This audit was conducted 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.

Audit Results

RMA found that, for the 20 core metrics, IAF's information security program was:

- Defined for six metrics,
- Consistently Implemented for five metrics, and
- Managed and Measurable for nine metrics.

Therefore, IAF's information security program was calculated by CyberScope[4] as overall Managed and Measurable. The following sections discuss each of these findings in more detail. See Appendix III for a summary of results for each core metric.

[4] CyberScope is a system that Federal agencies use to report their FISMA results.

IAF’s Implementation of Six Core Metrics Was Defined.
IAF’s implementation of its hardware inventory (metric 2), software inventory (metric 3), supply chain risk management (metric 14), secure configurations (metric 20), continuous monitoring (metric 47), and business impact analysis (metric 61) was defined. Therefore, its implementation of those six metrics was level 2.

Criteria for metric 2 states:

> …the organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization’s network and uses this taxonomy to inform which assets can/cannot be introduced into the network.

IAF did not maintain up-to-date hardware inventory records, as stated in its policies and procedures. Therefore, IAF’s implementation of its hardware inventory (metric 2) was defined (level 2).

Criteria for metric 3 states:

> …the organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for mobile applications, utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.

IAF did not maintain up-to-date software inventory records, as stated in its policies and procedures. Therefore, IAF’s implementation of its software inventory (metric 3) was defined (level 2).

Criteria for metric 14 states:

> …the organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain related risks associated with suppliers or contractors and the system, system component.
>
> In addition, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.
>
> Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.

IAF did not obtain assurance through audits, test results, or other forms of evaluation that the security of supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, IAF did not maintain visibility into its upstream suppliers and can consistently track changes in suppliers. As such, it did not consistently implement its supply chain risk management policies and procedures. Therefore, IAF's implementation of its supply chain risk management (metric 14) was defined (level 2).

Criteria for metric 20 states (among other things):

> The organization utilizes lessons learned in implementation to make improvements to its secure configuration policies and procedures.

IAF did not utilize lessons learned in implementation to make improvements to its secure configuration policies and procedures. Therefore, IAF's implementation of its secure configurations (metric 20) was defined (level 2).

Criteria for metric 47 states:

> …the organization's ISCM [information security continuous monitoring] policies and strategy are consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM policies and strategy.

IAF did not consistently capture lessons learned to make improvements to its ISCM strategy and policies. Therefore, IAF's implementation of its continuous monitoring (metric 47) was defined (level 2).

Criteria for metric 61 states:

> …the organization consistently incorporates the results of organizational and system level BIAs [business impact analysis] into strategy and plan development efforts.
>
> System level BIAs are integrated with the organizational level BIA and include characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.

IAF did not consistently use the results of its business impact analysis to determine mission essential functions and high-value assets as the BIA and continuity of operations plan referenced outdated information about unsupported hardware. Therefore, IAF's implementation of its business impact analysis (metric 61) was defined (level 2).

1. IAF's Implementation of Five Core Metric Was Consistently Implemented.

IAF's implementation of its authentication mechanisms for nonprivileged users (metric 30), data exfiltration (metric 37), workforce assessment (metric 42), incident detection and analysis (metric 54), and incident handling (metric 55) was consistently implemented.

Therefore, its implementation of those five metrics was level 3 and was, therefore, not effective.

Criteria for metric 30 states:

> …all non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points].

IAF's non-privileged users for one of the four selected systems did not utilize multi-factor mechanisms to authenticate to the applications. Therefore, IAF's implementation of its authentication mechanisms for nonprivileged users (metric 30) was consistently implemented (level 3).

Criteria for metric 37 states:

> …the organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware and blocks known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII [personally identifiable information]. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology and ensures the use of valid encryption certificates for its domains.

IAF did not complete the data exfiltration exercise during the audit period.[5] Therefore, IAF's implementation of its data exfiltration (metric 37) was consistently implemented (level 3).

Criteria for metric 42 states:

> …the organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.

IAF did not identify knowledge, skills, and abilities gaps through training or talent acquisition. Therefore, IAF's implementation of its workforce assessment (metric 42) was consistently implemented (level 3).

Criteria for metric 54 states:

> …the organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

[5] IAF is scheduled to complete the exercise in Q4 of FY 2022.

> The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.

IAF did not monitor and analyze qualitative and quantitative performance measures[6] on the effectiveness of its incident detection and analysis policies and procedures. Therefore, IAF's implementation of its incident detection and analysis (metric 54) was consistently implemented (level 3).

Criteria for metric 55 states:

> …the organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.
>
> The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

IAF did not monitor and analyze qualitative and quantitative performance measures[7] on the effectiveness of its incident detection and analysis policies and procedures. Therefore, IAF's implementation of its incident handling (metric 55) was consistently implemented (level 3).

2. IAF's Implementation of Nine Core Metric Was Managed and Measurable.

IAF's implementation of the following nine metrics was managed and measurable (level 4): 1, 5, 10, 21, 31, 32, 36, 49, and 63. Therefore, its implementation of those nine metrics was level 4.

For example, criteria for metric 21 states:

> …the organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.
>
> The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a

[6] The Continuous Diagnostics and Mitigation (CDM) dashboard is expected to provide this capability in FY 2023.

[7] The CDM dashboard is expected to provide this capability in FY 2023.

> reproducible format.
>
> …
>
> As part its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing.

IAF centrally manages its flaw remediation process and monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its flaw remediation processes as appropriate. However, as part of its flaw remediation processes, IAF did not perform a deeper analysis of software code, such as through patch sourcing and testing. Therefore, IAF's implementation of metric 21 was managed and measurable (level 4).

Also, criteria for metric 63 states:

> …the organization employs automated mechanisms to test system contingency plans more thoroughly and effectively.
>
> In addition, the organization coordinates plan testing with external stakeholders…as appropriate.
>
> …
>
> In addition, the organization proactively employs [organization defined mechanisms] to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes.

IAF employed automated mechanisms and coordinated plan testing with external stakeholders to test the contingency plan as appropriate. However, IAF did not proactively employ a mechanism to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes. Therefore, IAF's implementation of metric 63 was managed and measurable and was level 4.

Evaluation of Management Comments

In response to the draft report, IAF accepted the calculation of IAF’s information security program as managed and measurable. In addition, IAF will review the metrics assessed at the defined maturity level for possible remediation. IAF’s comments are included in their entirety in Appendix III.

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 conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objective. The audit was designed to determine the maturity level for the core FISMA metrics. It was not designed to determine causes of, effects of, or recommendations to improve the maturity levels.

The scope of this audit was to assess IAF's information security program consistent with FISMA reporting instructions issued by OMB and DHS. The audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *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
- 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 February 14, 2022. The audit also included a follow-up on seven prior audit recommendations associated with the core FISMA metrics to determine if IAF had made progress in implementing the recommended improvements concerning its information security program.[8] See Appendix II for the status of prior year recommendations.

Audit fieldwork covered IAF's headquarters located in Washington D.C., from March 23, 2022, to July 7, 2022. It covered the period from October 1, 2021 through July 7, 2022.

Methodology

To determine the IAF maturity level of the core metrics, RMA conducted interviews with IAF officials and contractors and reviewed the 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 reporting instructions issued by the OMB and DHS

[8] RMA only evaluated recommendation closure that would pertain to the core metrics. The remaining recommendations do not affect the core metrics and will be evaluated later.

and other requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls to determine the maturity levels of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations from FY 2021, 2020, 2019 & 2016.

In assessing the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them because the results did not need to be projected to the population. 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 Findings

The following table provides the status of the FY 2021, FY 2020, FY 2019, & FY2016 FISMA audit recommendations.[9][10][11][12][13]

Table 3: FY 2021, 2020, 2019 & 2016 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2022 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	Will be assessed later.
A-IAF-22-002-C (Rec.2)	Develop and implement supply chain risk management policies, procedures, and strategies	Closed	Disagree Refer to Audit Results - Metric 14
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	Will be assessed later.
A-IAF-22-002-C (Rec.4)	Approve and implement IAF's Information Resource Management Strategic Plan.	Closed	Agree
A-IAF-22-002-C (Rec.5)	Document and implement a procedure to approve IAF's table-top exercise plans before conducting the exercises.	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	Disagree Refer to Audit Results - Metrics 20 and 47
A-IAF-22-002-C (Rec.8)	Develop and implement an information security continuous monitoring strategy.	Closed	Will be assessed later.

[9] RMA only evaluated recommendation closure that would pertain to the core metrics. The remaining recommendations that do not affect the core metrics will be evaluated in FY 2023.

[10] 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)

[11] *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).

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

[13] *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).

Audit Report & Recommendation No.	FY 2022 Audit Recommendations	IAF’s Position	Auditor’s Position on the Status
A-IAF-22-002-C (Rec.9)	Develop and implement a written process to document participants in IAF's contingency plan training.	Closed	Will be assessed later.
A-IAF-17-004-C (Rec.7)	Implement multifactor authentication for all network accounts and document the results.	Closed	Agree
A-IAF-20-004-C (Rec.2)	Update the Continuity of Operations Plan to include a business impact analysis.	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	Disagree

Appendix III – Management Comments

INTER-AMERICAN FOUNDATION
EMPOWERED COMMUNITIES, SUSTAINABLE RESULTS

MEMORANDUM

TO: Alvin Brown, Deputy Assistant Inspector General for Audit

FROM: Lesley Duncan, Chief Operating Officer /s/

cc : Sara Aviel, President and Chief Executive Officer

DATE: August 18, 2022

SUBJECT: Inter-American Foundation (IAF) Response to the Office of Inspector General (OIG) Fiscal Year 2022 Federal Information Security Modernization Act (FISMA) Draft Audit Report (A-IAF-22-00X-C).

This memorandum provides Inter-American Foundation (IAF)'s management comments for the aforementioned draft audit, dated August 12, 2022.

The scope of this audit was to assess whether IAF's information security program was consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit objective was to determine the maturity level IAF achieved for each of its core FISMA reporting metrics. Therefore, it was not designed to determine causes of, effects of, or make recommendations to improve the maturity levels.

The auditors concluded that, for the 20 core metrics, IAF's information security program was managed and measurable for 9 metrics, consistently implemented for 5 metrics, and defined for 6 metrics. The IAF's information security program was calculated as managed and measurable.

The IAF accepts the calculation of the auditors, appreciates the engagement opportunity and will review metrics designated with maturity level of defined for remediation, as possible.

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 202-688-3047 or lduncan@iaf.gov.

Appendix IV – Summary Results of Each Core Metric

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
1. FY22 Core Metric: To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?				☒	
2. FY22 Core Metric: To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?		☒			
3. FY22 Core Metric: To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?		☒			
5. FY22 Core Metric: To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?				☒	

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
10. FY22 Core Metric: To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?				☒	
14. FY22 Core Metric: To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?		☒			
20. FY22 Core Metric: To what extent does the organization utilize settings/common secure configurations for its information systems?		☒			
21. FY22 Core Metric: To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?				☒	
30. FY22 Core Metric: To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for nonprivileged users to access the organization's facilities [organization defined entry/exit points], networks, and systems, including for remote access?			☒		

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
31. <u>FY22 Core Metric:</u> To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?				☒	
32. <u>FY22 Core Metric:</u> To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?				☒	
36. <u>FY22 Core Metric:</u> To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?				☒	
37. <u>FY22 Core Metric:</u> To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?			☒		

Metric	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
42. FY22 Core Metric: To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?			☒		
47. FY22 Core Metric: To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?		☒			
49. FY22 Core Metric: How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?				☒	
54. FY22 Core Metric: How mature are the organization's processes for incident detection and analysis?			☒		
55. FY22 Core Metric: How mature are the organization's processes for incident handling?			☒		
61. FY22 Core Metric: To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?		☒			
63. FY22 Core Metric: To what extent does the organization perform tests/exercises of its information system contingency planning processes?				☒	
Total	**0**	**6**	**5**	**9**	**0**