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

# 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


Information Technology Audits Division

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

# MEMORANDUM

**DATE:** November 19, 2021

**TO:** Inter-American Foundation, Interim President and Chief Executive Officer, Lesley Duncan

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

**SUBJECT:** IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-IAF-22-002-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF's) information security program for fiscal year 2021, 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 the audit firm to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed the audit firm's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on IAF's compliance with FISMA. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which RMA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether IAF implemented an effective information security program.[1] To answer the audit objective, RMA evaluated the effectiveness of IAF's implementation of the FY 2021 Inspector General (IG) FISMA metrics[2] that fall into the nine domains in the following table. Also, RMA assessed IAF's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

[1] 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.
[2] Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," May 12, 2021.

RMA reviewed four of five systems in IAF's inventory dated February 16, 2021. Audit fieldwork covered IAF's headquarters in Washington, DC, from April 2, 2021, to August 26, 2021, for the period from October 1, 2020, through August 26, 2021.

Although the table below shows that RMA noted weaknesses in all nine FY 2021 IG FISMA metric domains, the audit firm concluded that IAF generally implemented an effective information security program. This conclusion is based on IAF's overall implementation of security controls as a whole and considering the unique mission, resources, and challenges of IAF. For example, IAF:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured that its information system backup and storage processes are assessed as part of its continuous monitoring program.
- Maintained an accurate inventory of hardware and software assets.

Nonetheless, RMA identified weaknesses. Eight domains were affected by a weakness that IAF did not create a monitoring plan to review its policies and procedures. In addition, five domains were affected by a weakness that IAF did not conduct and document the lessons learned.

| **Fiscal Year 2021 IG FISMA Metric Domains** | **Weaknesses Identified** |
|---|---|
| Risk Management | X |
| Supply Chain Risk Management | X |
| Configuration Management | X |
| Identity and Access Management | X |
| Data Protection and Privacy | X |
| Security Training | X |
| Information Security Continuous Monitoring | X |
| Incident Response | X |
| Contingency Planning | X |

To address the weaknesses identified in RMA's report, we recommend that IAF's chief information officer take the following actions:

**Recommendation 1.** 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.

**Recommendation 2.** Develop and implement supply chain risk management policies, procedures, and strategies.

**Recommendation 3.** Develop and implement a procedure to document risk acceptance when vulnerabilities cannot be remediated within the timeframes specified in IAF's operating procedures.

**Recommendation 4.** Approve and implement IAF's Information Resource Management Strategic Plan.

**Recommendation 5.** Document and implement a procedure to approve IAF's table-top exercise plans before conducting the exercises.

**Recommendation 6.** Document and implement a written process for obtaining and evaluating feedback on IAF's privacy and security training content, including role-based training.

**Recommendation 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.

**Recommendation 8.** Develop and implement an information security continuous monitoring strategy.

**Recommendation 9.** Develop and implement a written process to document participants in IAF's contingency plan training.

In addition, IAF had not taken final corrective action on three recommendations from the FY 2016,[3] FY 2019[4] and FY 2020[5] FISMA audits. Refer to Appendix II on page 21 of RMA's report for the status of prior year recommendations.

In finalizing the report, the audit firm evaluated IAF's responses to the recommendations. After reviewing that evaluation, we consider all nine recommendations resolved but open pending completion of planned activities. For the nine recommendations, 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.

[3] Recommendation 7 in "The Inter-American Foundation Has Implemented Many Controls in Support of FISMA, But Improvements are Needed" (Audit Report No. A-IAF-17-004-C, November 7, 2016).
[4] Recommendation 2 in "IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019" (Audit Report No. A-IAF-20-004-C, January 23, 2020).
[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).


# Inter-American Foundation (IAF)

Federal Information Security Modernization Act of 2014
(FISMA)

Final Report
Fiscal Year 2021

RMA | Associates
Auditors. Consultants. Advisors.

November 19, 2021

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 2021.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and that of IAF. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Respectfully,

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

RMA | Associates
Auditors. Consultants. Advisors.

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

November 19, 2021

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 whether IAF's information security program was consistent with FISMA 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 Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated January 22, 2015.

For this audit, we reviewed four of five judgmentally selected systems in IAF's inventory as of February 16, 2021. Audit fieldwork covered IAF's headquarters located in Washington, DC, from April 2, 2021, to August 26, 2021.

Our audit was conducted 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 all nine Inspector General FISMA Metric Domains mostly due to a monitoring plan not being created to review its policies and procedures and lessons learned not being conducted and documented. We made nine recommendations to assist IAF in strengthening its information security program. In addition, three recommendations related to prior year findings were not fully implemented.

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 ..... 6
1. IAF Needs to Fully Document the Business Reason and Compensating Controls When Accepting the Risk for Known Vulnerabilities. ..... 6
2. IAF Needs to Document and Implement Supply Chain Risk Management Policies, Procedures, and Strategy. ..... 7
3. IAF Needs to Remediate Vulnerabilities Within the IAF Defined Remediation Timeframe. … ..... 8
4. IAF Needs to Approve and Implement its Information Resource Management Strategic Plan. ..... 9
5. IAF Needs to Implement Multi-Factor Authentication for Non-Privileged Accounts. ..... 10
6. IAF Needs to Approve its Table-Top Exercise Plan for Data Breach. ..... 11
7. IAF Needs to Collect Feedback on the Content of its Security and Privacy Training. ..... 12
8. IAF Needs to Fully Conduct and Document Lessons Learned. ..... 12
9. IAF Needs to Develop and Implement an Information Security Continuous Monitoring Strategy. ..... 13
10. IAF Needs to Update the Continuity of Operations Plan to Include a Business Impact Analysis. ..... 15
11. IAF Needs to Document That Contingency Training Was Provided to Personnel Who Have Contingency Roles and Responsibilities. ..... 15
12. IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures. ..... 17
Evaluation of Management Comments ..... 18
Appendix I – Scope and Methodology ..... 19
Scope ..... 19
Methodology ..... 20
Appendix II - Status of Prior Year Findings ..... 21
Appendix III – Management Comments ..... 22

## 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) 2021. 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).

Annually, OMB and the Department of Homeland Security provide instructions to Federal agencies and IGs for assessing agency information security programs. On November 9, 2020, OMB issued OMB Memorandum M-21-02, "*Fiscal Year 2020-2021 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 2021 metrics are designed to assess the maturity[4] 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.

---

[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 was defined as having an overall mature program based on the current year Inspector General FISMA reporting metrics.

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

[4] The five maturity levels 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 2021 IG FISMA Metric Domains*

| Cybersecurity Framework Security Functions | FY 2021 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 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. RMA believes 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, based on IAF's overall implementation of security controls and considering the unique mission, resources, and challenges of IAF. For example, IAF:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Ensured that its information system backup and storage processes are assessed as part of its continuous monitoring program.
- Maintained an accurate inventory of hardware and software assets.

The overall maturity level of IAF's information security program was Consistently Implemented. We have presented the maturity level for each of the nine domains below:

*Table 2: FY 21 IAF Maturity Level*

| Cybersecurity Framework Security Functions | FY 2021 IG FISMA Metric Domains | Maturity Level |
|---|---|---|
| Identify | Risk Management | Consistently Implemented |
| Identify | Supply Chain Risk Management[5] | Ad Hoc |
| Protect | Configuration Management | Defined |
| Protect | Identity and Access Management | Consistently Implemented |
| Protect | Data Protection and Privacy | Consistently Implemented |

[5] To provide agencies with sufficient time to implement NIST SP 800-53 Revision 5, the SCRM domain was not used to calculate the Identify framework function rating or the overall maturity level.

| Cybersecurity Framework Security Functions | FY 2021 IG FISMA Metric Domains | Maturity Level |
|---|---|---|
| Protect | Security Training | Consistently Implemented |
| Detect | Information Security Continuous Monitoring | Consistently Implemented |
| Respond | Incident Response | Consistently Implemented |
| Recover | Contingency Planning | Managed and Measurable |
| **Overall** | | **Consistently Implemented** |

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 all nine IG FISMA Metric Domains (Table 3) and presented recommendations to strengthen the agency's information security program. We noted that eight of the domains had weaknesses related to the monitoring plan not being created to review its policies and procedures and five domains had weaknesses related to lessons learned not being conducted and documented.

*Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2021 FISMA Assessment*

| Cybersecurity Framework Security Functions | FY 2021 IG FISMA Metric Domains | Weakness Noted in FY 2021 |
|---|---|---|
| Identify | Risk Management | IAF Needs to Fully Document the Business Reason and Compensating Controls When Accepting the Risk for Known Vulnerabilities (Finding 1).<br><br>IAF Needs to Fully Conduct and Document Lessons Learned (Finding 8).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |
| Identify | Supply Chain Risk Management | IAF Needs to Document and Implement Supply Chain Risk Management Policies, Procedures, and Strategy (Finding 2). |
| Protect | Configuration Management | IAF Needs to Remediate Vulnerabilities Within the IAF Defined Remediation Timeframe (Finding 3).<br><br>IAF Needs to Fully Conduct and Document Lessons Learned (Finding 8).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |

| Cybersecurity Framework Security Functions | FY 2021 IG FISMA Metric Domains | Weakness Noted in FY 2021 |
|---|---|---|
| Protect | Identity and Access Management | IAF Needs to Approve and Implement its Information Resource Management Strategic Plan (Finding 4).<br><br>IAF Needs to Implement Multi-Factor Authentication for Non-Privileged Accounts (Finding 5).<br><br>IAF Needs to Fully Conduct and Document Lessons Learned (Finding 8).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |
| Protect | Data Protection and Privacy | IAF Needs to Approve its Table-Top Exercise Plan for Data Breach (Finding 6).<br><br>IAF Needs to Collect Feedback on the Content of its Security and Privacy Training (Finding 7).<br><br>IAF Needs to Fully Conduct and Document Lessons Learned (Finding 8).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |
| Protect | Security Training | IAF Needs to Collect Feedback on the Content of its Security and Privacy Training (Finding 7).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |
| Detect | Information Security Continuous Monitoring | IAF Needs to Fully Conduct and Document Lessons Learned (Finding 8).<br><br>IAF Needs to Develop and Implement an Information Security Continuous Monitoring Strategy (Finding 9).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and |

| Cybersecurity Framework Security Functions | FY 2021 IG FISMA Metric Domains | Weakness Noted in FY 2021 |
|---|---|---|
| | | Procedures (Finding 12). |
| Respond | Incident Response | IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |
| Recover | Contingency Planning | IAF Needs to Update the Continuity of Operations Plan to Include a Business Impact Analysis (Finding 10).<br><br>IAF Needs to Document That Contingency Training Was Provided to Personnel Who Have Contingency Roles and Responsibilities. (Finding 11).<br><br>IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures (Finding 12). |

We are making nine new recommendations to address the weaknesses identified. In response to the draft report, IAF outlined and described its plans to address all nine recommendations. Based on our evaluation of management comments, we acknowledge IAF's management decision on all nine recommendations. Further, we consider these recommendations resolved, but open pending completion of planned activities. IAF's comments are included in their entirety in Appendix III.

In addition, as illustrated in Appendix II, IAF took corrective action to address one prior year recommendation, but three prior-year recommendations were not fully implemented. Appendix I describes the audit scope and methodology. Detailed findings appear in the following section.

## Audit Findings

### 1. IAF Needs to Fully Document the Business Reason and Compensating Controls When Accepting the Risk for Known Vulnerabilities.

**Cybersecurity Framework Security Function:** *Identify*
**FY21 IG FISMA Metric Domain:** *Risk Management*

IAF developed a risk acceptance form as required by IAF's risk tolerance and risk strategy. However, the form did not provide sufficient information for risk acceptance and the compensating controls implemented to reduce the risks of exploitation.

NIST Special Publication (SP) 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* states:

> **TASK 3-1:** Identify alternative courses of action to respond to risk determined during the risk assessment.
>
> Supplemental Guidance: Organizations can respond to risk in a variety of ways. These include: (i) risk acceptance; (ii) risk avoidance; (iii) risk mitigation; (iv) risk-sharing; (v) risk transfer; or (vi) a combination of the above. A course of action is a time-phased or situation-dependent combination of risk response measures.
>
> **TASK 3-3:** Decide on the appropriate course of action for responding to risk.
>
> Supplemental Guidance: A key part of the risk decision process is the recognition that regardless of the decision, there still remains a degree of residual risk that must be addressed. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance and the specific risk tolerances of particular decision makers.

According to IAF officials, prior to approving the risk acceptance form for agency use, the Chief Operating Officer, Chief Information Officer (CIO), and Chief Information Security Officer discussed industry-leading practices which would justify risk acceptance and applicable justification and compensating controls if any. However, the newly created risk acceptance form did not fully capture the process used to determine whether the risk exceeded an acceptable level.

Without fully documenting the process, IAF may inadvertently accept risks that exceeded IAF's risk tolerance levels and may have risks that IAF did not consider while determining an acceptable level.

***Recommendation 1:*** *We recommend that IAF's Chief Information Officer 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.*

## 2. IAF Needs to Document and Implement Supply Chain Risk Management Policies, Procedures, and Strategy.

**Cybersecurity Framework Security Function:** *Identify*
**FY21 IG FISMA Metric Domain:** *Supply Chain Risk Management*

IAF did not document and implement policies, procedures, and strategies to address supply chain risk management.

Public law 115-390 – 115th Congress, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "SECURE Technology Act" (December 31, 2018) requires executive agencies to develop an overall SCRM strategy and implementation plan and policies and processes to guide and govern SCRM activities.

In addition, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Chapter 2, section 2.2.1 FRAME, states:

> An organization Information and Communication Technology (ICT) SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency's Risk Management Process and System Development Life Cycle (SDLC).

According to IAF officials, supply chain risk management is a new domain in the FY 2021 IG FISMA Reporting Metrics and required controls were stated in the latest NIST SP 800-53 Revision 5, published in September 2020. IAF has one year to implement supply chain risk management related controls to be compliant.

Without supply chain risk management policies, procedures, and strategies, IAF may not adequately consider security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy. It can guide and inform supply chain policies and system-level supply chain risk management plans.

***Recommendation 2:*** *We recommend that IAF's Chief Information Officer develop and implement supply chain risk management policies, procedures, and strategies.*

## 3. IAF Needs to Remediate Vulnerabilities Within the IAF Defined Remediation Timeframe.

**Cybersecurity Framework Security Function:** *Protect*
**FY21 IG FISMA Metric Domain:** *Configuration Management*

IAF did not remediate its vulnerabilities within the IAF defined timeframe. We identified 45 critical vulnerabilities, 689 high vulnerabilities, 171 moderate vulnerabilities, and 3 low vulnerabilities that were not remediated in accordance with the timeframes in IAF's standard operating procedures.

IAF's Information System Security Program Standard Operating Procedures Vulnerability Management Process (April 2021) states:

> 3. Prioritize & Remediate
>
> Perform patching activities by the following risk priority schedule:
> - Critical/High Vulnerabilities: 30-day remediation
> - Moderate Vulnerabilities: 60-day remediation
> - Low Vulnerabilities: 120-day remediation

In addition, NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations states:

> **Sl-2 FLAW REMEDIATION**
>
> Control: The organization:
> a. identifies, reports, and corrects information system flaws;
> b. tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
> c. installs security-relevant software and firmware updates within [*Assignment: organization-defined period*] of the release of the updates; and
> d. incorporates flaw remediation into the organizational configuration management process.

According to IAF officials, some patches were not yet developed by the software and hardware vendors. Other times, IAF needed additional time to test the patches before implementing them. Moreover, IAF had been in a remote work status since March 2020, which delayed the ability to deploy patches and mitigate vulnerabilities.

Nonetheless, IAF did not consistently implement its procedures to remediate vulnerabilities within the specified timeframes. Further, IAF did not have a procedure to document a risk acceptance for deviating from its policy.

Not promptly remediating known vulnerabilities increases the risk that mission information or other sensitive data may be inadvertently or deliberately misused. Such misuse may result in improper information disclosure, manipulation, or theft. Additionally, uncorrected

vulnerabilities may lead to inappropriate or unnecessary changes to mission-focused information systems, resulting in compromising mission information or other sensitive data.

***Recommendation 3:*** *We recommend that IAF's Chief Information Officer develop and implement a procedure to document risk acceptance when vulnerabilities cannot be remediated within the timeframes specified in the agency's operating procedures.*

## 4. IAF Needs to Approve and Implement its Information Resource Management Strategic Plan.

**Cybersecurity Framework Security Function:** *Protect*
**FY21 IG FISMA Metric Domain:** *Identity and Access Management*

IAF's Information Resource Management Strategic Plan was revised in March 2021. However, IAF's plan was not approved and implemented.

NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* states:

> **AC-1 ACCESS CONTROLS POLICIES AND PROCEDURES**
>
> Control: The organization:
> a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
>  1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
>  2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
>
> b. Reviews and updates the current:
>  1. Access control policy [*Assignment: organization-defined frequency*]; and
>  2. Access control procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53, Revision 4*, further* states:

> **RM-9 RISK MANAGEMENT STRATEGY**
>
> Control: The organization:
> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
> b. Implements the risk management strategy consistently across the organization; and
> c. Reviews and updates the risk management strategy [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

According to IAF officials, IAF was in the process of approving the Information Resource Management Strategic Plan but had not completed its internal review process. As a result, IAF did not approve and implement the plan.

Without an approved Information Resource Management Strategic Plan, IAF cannot effectively integrate and focus its people, technology, and operations towards achieving IAF's Information Resource Management goals. In addition, the agency's security practices may deviate from policies and procedures over time. Further, security practices are at risk of becoming misunderstood and improperly implemented.

***Recommendation 4:*** *We recommend that IAF's Chief Information Officer approve and implement its Information Resource Management Strategic Plan.*

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

**Cybersecurity Framework Security Function:** *Protect*
**FY21 IG FISMA Metric Domain:** *Identity and Access Management*

IAF did not implement strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access IAF's networks and systems. Multifactor authentication for non-privileged users was only implemented for remote access. As such, IAF will not be fully PIV compliant until all its information systems (applications) can be accessed only via PIV authentication in lieu of a username and password.

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

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

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

IAF's information technology equipment was capable of accepting PIV cards. However, according to IAF officials, due to limited resources and competing priorities, IAF did not employ sufficient resources to fully comply with OMB M-11-11.

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

A recommendation addressing this finding was issued in the FY 2016 FISMA audit report.[6] Because that recommendation is still open, we are not making a new recommendation at this time.

## 6. IAF Needs to Approve its Table-Top Exercise Plan for Data Breach.

**Cybersecurity Framework Security Function:** *Protect*
**FY21 IG FISMA Metric Domain:** *Data Protection and Privacy*

IAF conducted a table-top exercise for Data Breach on March 3, 2021. However, the plan to conduct a table-top exercise was not approved for use.

OMB M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, section X. Tabletop Exercises and Annual Plan Reviews, states:

> A. Table-top Exercises
>
> The Senior Agency Official Privacy (SAOP) shall periodically, but not less than annually, convene the agency's breach response team to hold a table-top exercise. The purpose of the table-top exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing breach response plans is an essential part of risk management and breach response preparation. Table-top exercises should be used to practice a coordinated response to a breach, further refine and validate the breach response plan, and identify potential weaknesses in an agency's response capabilities.

The Chief Information Officer conducted the table-top exercises; however, due to management oversight, the CIO did not approve its table-top exercise for use. Further, IAF did not have a procedure to approve its plan for conducting table-top exercises.

By not approving a table-top exercise for the data breach, IAF may not disseminate the results of its table-top exercise to the appropriate stakeholders.

***Recommendation 5:*** *We recommend that IAF's Chief Information Officer document and implement a procedure to approve its table-top exercise plans before conducting the exercises.*

[6] Recommendation 7 in *The Inter-American Foundation Has Implemented Many Controls in Support of FISMA But Improvements are Needed.* (Audit Report No. A-IAF-17-004-C, November 7, 2016).

## 7. IAF Needs to Collect Feedback on the Content of its Security and Privacy Training.

**Cybersecurity Framework Security Function:** *Protect*
**FY21 IG FISMA Metric Domain:** *Data Protection and Privacy, and Security Training*

IAF uses the Department of Defense Cyber Awareness Challenge Training for its annual security awareness and basic privacy awareness training. In addition, IAF uses third-party vendors for its role-based privacy and security training. However, IAF management did not collect documented feedback from its users on the training content.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), states:

> **6.2 Evaluation and Feedback**
> Formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program.

IAF's training program is adjusted each year as the master training materials are updated by the Department of Defense and the third-party vendor. As a result, IAF did not believe it was necessary to collect formal feedback from its users. As such, IAF did not have a process to obtain and evaluate feedback.

IAF cannot determine what updates are needed to its security and privacy training unless feedback is collected from its users. Also, if improvement in training programs is not made, it may not prepare users to avoid cybersecurity compromises.

***Recommendation 6:*** *We recommend that IAF's Chief Information Officer document and implement a written process for obtaining and evaluating feedback on its privacy and security training content, including role-based training.*

## 8. IAF Needs to Fully Conduct and Document Lessons Learned.

**Cybersecurity Framework Security Function:** *Identity, Protect, and Detect*
**FY21 IG FISMA Metric Domain:** *Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Information Security Continuous Monitoring*

IAF lacked a formal, disciplined lesson learned process for the following FISMA Functions and Domains:

- Identify (Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)

- Protect (Data Protection and Privacy)
- Detect (Information Security Continuous Monitoring)

NIST *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 states:

> Functions organize basic cybersecurity activities at their highest level. These functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.
>
> Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

In addition, NIST SP 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, states:

> …to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high-impact systems. Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems.

IAF management believed that their weekly meeting was an adequate process to discuss lessons learned and any issues or concerns; however, IAF did not have a process to document the discussions that were held during the weekly meeting.

Without a written lesson learned process, IAF may not capture information from previous practices to identify areas for improvements. Therefore, IAF loses the opportunity to strengthen its security posture against actual risk events.

***Recommendation 7:*** *We recommend that IAF's Chief Information Officer 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 its security posture.*

## 9. IAF Needs to Develop and Implement an Information Security Continuous Monitoring Strategy.

**Cybersecurity Framework Security Function:** *Detect*
**FY21 IG FISMA Metric Domain:** *Information System Continuous Monitoring*

IAF uses the shared service of the Cybersecurity and Infrastructure Security Agency (CISA). The memorandum of agreement (MOA) between the agencies provided an overview of the Continuous Diagnostics and Monitoring strategy and process. Even though IAF had an MOA with CISA, it does not replace the need for an ISCM

strategy. For example, the MOA did not address IAF's risk tolerance, the establishment of IAF-defined metrics, its visibility into the security of the assets, and awareness of threats and vulnerabilities.

NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* states:

> **CA -7 CONTINUOUS MONITORING**
>
> Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
> a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;
> b. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;

In addition, OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, Appendix I, section 4, Specific Requirements, states that agencies shall:

> 5) Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers;
> 6) Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls; significant changes to information systems; and adherence to Federal statutes, policies, directives, instructions, regulations, standards, and guidelines;

According to IAF officials, IAF believed existing ISCM resources, policies, and procedures were sufficient to address all the aspects of the strategy; as such, IAF did not develop an ISCM strategy.

Without a formal ISCM strategy, IAF may not ensure that compromises to the security architecture are managed to prevent or minimize the impact on business and mission functions.

***Recommendation 8:*** *We recommend that IAF's Chief Information Officer develop and implement an information security continuous monitoring strategy.*

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

**Cybersecurity Framework Security Function:** *Recover*
**FY21IG FISMA Metric Domain:** *Contingency Planning*

IAF's Continuity of Operations Plan (COOP) dated July 2021 did not fully address maintaining business functions, which would be addressed in the business impact analysis[7] (BIA).

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

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

IAF revised its BIA in August 2021; however, due to limited resources and competing priorities, IAF did not incorporate the BIA into its COOP.

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

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit report.[8] Because that recommendation is still open, we are not making a new recommendation at this time.

## 11. IAF Needs to Document That Contingency Training Was Provided to Personnel Who Have Contingency Roles and Responsibilities.

**Cybersecurity Framework Security Function:** *Recover*
**FY21 IG FISMA Metric Domain:** *Contingency Planning*

On April 9, 2021, IAF conduced a table-top exercise of its contingency plan, which IAF officials said was also contingency plan training. However, IAF did not have evidence, such as a sign-in sheet, that all contingency personnel participated.

[7] A BIA is an analysis of its information technology system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of significant disruption.
[8] Recommendation 2 in *IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-IAF-20-004-C, January 23, 2020).

NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* states*:*

**CP-3 CONTINGENCY TRAINING**

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites, and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

In addition, NIST SP 800-34, Revision 1*, Contingency Planning Guide for Federal Information Systems* states:

**3.5.2 Training**

Training should be provided at least annually. Personnel newly appointed to Information System Contingency Plan (ISCP) roles should receive training shortly thereafter. Ultimately, ISCP personnel should be trained to the extent that they are able to execute their respective recovery roles and responsibilities without the aid of the actual ISCP document.

IAF did not have a process in place to document the participants of its contingency planning training to ensure all individuals with contingency planning responsibilities participated in the annual contingency plan exercise.

Without ensuring contingency training is provided for individuals with contingency plan responsibilities, the ISCP personnel may not be prepared to participate in test/exercises as well as actual outage events.

***Recommendation 9:*** *We recommend that IAF's Chief Information Officer develop and implement a written process to document participants in the agency's contingency plan training.*

## 12. IAF Needs to Create a Monitoring Plan to Review Its Policies and Procedures.

**Cybersecurity Framework Security Function:** *All Functions*
**FY21 IG FISMA Metric Domain:** *Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning*

IAF did not develop a monitoring plan to address the recommendation made in FY 20 FISMA audit. Although, IAF updated its policies and procedures, they did not implement a monitoring plan to make sure policies and procedures do not deviate from the agency's security practices and Federal guidance.

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

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

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

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

A recommendation addressing this finding was issued in the fiscal year 2020 FISMA audit report.[9] Because that recommendation is still open, we are not making a new recommendation at this time.

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

## Evaluation of Management Comments

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

Based on our evaluation of management comments, we acknowledge IAF's management decisions on all nine recommendations. Further, we consider these recommendations 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. The audit was designed to determine whether IAF had 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 OMB and the Department of Homeland Security. In addition, the audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed IAF's performance and compliance with FISMA in the following areas:

- Risk Management
- 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 five judgmentally selected systems in IAF's inventory as of February 16, 2021. The audit also included a follow-up on four prior audit recommendations[10][11][12] to determine if IAF had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for status or prior year recommendations.

Audit fieldwork covered IAF's headquarters located in Washington, DC, from April 2, 2021, to August 26, 2021. It covered the period from October 1, 2020, through August 26, 2021.

[10] Recommendation 7 in *The Inter-American Foundation Has Implemented Many Controls in Support of FISMA But Improvements are Needed.* (Audit Report No. A-IAF-17-004-C, November 7, 2016).
[11] Recommendation 2 in *IAF Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-IAF-20-004-C, January 23, 2020).
[12] Recommendations 1 and 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).

**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 to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations for FY 2016, FY 2019, and FY 2020.

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 Findings

The following table provides the status of the FY 2016, FY 2019, and FY 2020 FISMA audit recommendations.[13][14][15]

*Table 4: FY 2016, 2019, & 2020 FISMA Audit Recommendations*

| Audit Report & Recommendation No. | FY 2016, 2019, & 2020 Audit Recommendations | IAF's Position | Auditor's Position on the Status |
|---|---|---|---|
| A-IAF-17-004-C (Rec.7) | Implement multifactor authentication for all network accounts and document the results. | Open | Agree. See finding 5 |
| A-IAF-20-004-C (Rec.2) | Update the Continuity of Operations Plan to include a business impact analysis. | Open | Agree. See finding 10 |
| A-IAF-21-002-C (Rec.1) | Develop and implement policies and procedures related to POA&Ms to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to extend estimated completion dates and determine the dependencies and completion of milestones that affect the estimated due dates to ensure that they are met. | 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. | Open | Agree. See finding 12 |

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


**MEMORANDUM**

**TO:** Alvin A. Brown, Deputy Assistant Inspector General for Audit, USAID OIG

**CC:** Chris Wood, Interim COO, Inter-American Foundation

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

**SUBJECT:** Update, Plan and Action on Recommendations from USAID OIG Draft Audit Report No. A-IAF-22-00X-C dated October 20, 2021

This memorandum provides actions planned and undertaken to address the recommendations contained in the Audit of the Inter-American Foundation's (IAF) Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2021, Audit Report A-IAF- 22-00X-C, dated October 20, 2021.

**Recommendation 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.**

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

- Update the IAF Vulnerability Management Process within the IAF Information System Security Program Standard Operating Procedures (SOP) in regards to risk acceptance actions and requirements.
- Update IAF Risk Acceptance Form to include documented business reason for risk acceptance, compensating controls implemented to reduce risk, and approval by the System Owner and Authorizing Official.

Target date: 12/31/2021

**Recommendation 2. Develop and implement supply chain risk management policies, procedures, and strategies.**

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

b. Develop and implement a supply chain risk management program to include:
    - Update the IAF Information Security Manual (ISM) with supply chain risk management policies in accordance with NIST Special Publication (SP) 800-53, Rev 5, "*Security and Privacy Controls for Information Systems and Organizations*."
    - Update the IAF Information System Security Program Standard Operating Procedures (SOP) to establish supply chain risk management processes and procedures.
    - Develop and document an agency Supply Chain Risk Management (SCRM) strategic plan.

c. Implement the SCRM program in Q4.

Target date: 03/31/2022

**Recommendation 3. Develop and implement a procedure to document risk acceptance when vulnerabilities cannot be remediated within the timeframes specified in IAF's operating procedures.**

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

a. Provide additional oversight to facilitate and manage the prioritization and remediation of vulnerabilities and Plan of Action and Milestone items within designated timeframes per the risk priority schedule designated in the IAF Vulnerability Management Process.
b. Develop a waiver request process and form for non-compliance with IAF policy to ensure that an acceptable plan to remediate the weakness has been provided and compensating controls have been implemented.
c. Update risk acceptance actions and requirements within the IAF Vulnerability Management Process when vulnerabilities or material weaknesses cannot be remediated within designated timeframes.
d. Manage and review all authorized risk acceptance requests annually.

Target date: 12/31/2021

**Recommendation 4. Approve and implement IAF's Information Resource Management Strategic Plan.**

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

a. Finalize the IAF Information Resource Management Strategic Plan.
b. Approve the plan and have it authorized/signed by the COO.

Target date: 12/31/2021

**Recommendation 5. Document and implement a procedure to approve IAF's table-top exercise plans before conducting the exercises.**

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

a. Update the IAF Information System Security Program Standard Operating Procedures (SOP) to include approval/acceptance of any scheduled training or table-top exercise plan and/or Lessons Learned report.
b. Update the IAF Table Top Exercise Plan and Lessons Learned template with designated IAF personnel approval signatures.

Target date: 12/31/2021

**Recommendation 6. Document and implement a written process for obtaining and evaluating feedback on IAF's privacy and security training content, including role-based training.**

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

a. Develop a security awareness and training evaluation form to periodically collect feedback on agency training results.
b. Update the IAF Information System Security Program Standard Operating Procedures (SOP) to include a new training feedback process for security awareness and role-based training results.
c. Solicit security awareness training feedback from a representative list of employees periodically.

Target date: 12/31/2021

**Recommendation 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.**

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

a. Develop a new "Lessons Learned" process form aligned with the five functional areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).
b. Update the IAF Information System Security Program Standard Operating Procedures (SOP) to include a "lessons learned" process related to the following FISMA functions:
    - Identify (Risk Management)
    - Protect (Configuration Management)
    - Protect (Identity & Access Management)

- Protect (Data Protection and Privacy)
- Detect (Information Security Continuous Monitoring)

Target date: 03/31/2022

**Recommendation 8. Develop and implement an information security continuous monitoring strategy.**

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

a. Develop and formally document an information security continuous monitoring (ISCM) strategy plan.
b. Approve and implement the ISCM Plan.

Target date: 12/31/2021

**Recommendation 9. Develop and implement a written process to document participants in IAF's contingency plan training.**

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

a. Update the IAF Information System Security Program Standard Operating Procedures (SOP) to include a process to document participants in the training.
b. Update the IAF Table Top Exercise Plan and Lessons Learned template with an "Attendees" section to document participants with digital signature acknowledgement.

Target date: 12/31/2021