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

FISMA: Effectiveness of IAF's Information Security Program for FY 2025 Could Not Be Determined and Weaknesses Continue to Exist

Report A-IAF-26-003-M
February 24, 2026

Evaluation

Office of Audits, Inspections, and Evaluations

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

DATE: February 24, 2026

TO: Sara Aviel
President and Chief Executive Officer
Inter-American Foundation

FROM: Gabriele Tonsil /s/
Acting Assistant Inspector General for Audits, Inspections, and Evaluations

SUBJECT: FISMA: Effectiveness of IAF's Information Security Program for FY 2025 Could Not Be Determined and Weaknesses Continue to Exist

This memorandum transmits the final report on our evaluation of the Inter-American Foundation's (IAF) information security program for fiscal year (FY) 2025, in support of the Federal Information Security Modernization Act of 2014 (FISMA). Our objective was to determine whether IAF implemented an effective information security program. In finalizing the report, we considered your comments on the draft and included them in their entirety in Appendix C.

The report contains six new recommendations to improve IAF's information security program. In addition, it identifies two recommendations from our prior FISMA audits that remain open. After reviewing information you provided in response to the draft report, we consider the six new recommendations resolved but open pending completion of planned activities. For all recommendations, please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance you and your staff provided to us during this engagement.

Contents

Office of Inspector General
U.S. Agency for International Development

Report No A-IAF-26-003-M
February 24, 2026

Report in Brief

Why We Did This Evaluation

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agency systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems. The statute requires agency heads to implement policies and procedures to protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. The act also directs the USAID Office of Inspector General to conduct an annual independent assessment of the Inter-American Foundation's (IAF) information security programs and practices and report the results of the assessments to the Office of Management and Budget.

We conducted this evaluation to determine whether IAF implemented an effective information security program. We focused on IAF's information security program for fiscal year (FY) 2025 as of June 20, 2025, to ensure that we met the deadline to provide the results of our assessment to the Agency. Following the February 19, 2025, executive order, "Commencing the Reduction of the Federal Bureaucracy," IAF's staffing was significantly reduced, and many Agency personnel were placed on administrative leave.

What We Recommend

We made six recommendations to strengthen the effectiveness of IAF's information security program. In addition, we referenced two recommendations from our 2024 FISMA audit that the Agency has not yet implemented.

What We Found

OIG could not determine the overall effectiveness of IAF's information security program in FY 2025. However, the Agency met requirements for certain areas. For example, the Agency adhered to supply chain policies and procedures, established requirements for monitoring security incidents, and tested contingency plans. IAF also implemented two of our four prior recommendations. However, we identified multiple weaknesses.

IAF has continued challenges in timely remediating critical vulnerabilities. In addition, the Agency has not implemented a related prior recommendation. This makes it easier for attackers to exploit weaknesses by executing malicious code, stealing data, or compromising staff's access to systems.

IAF has not fully implemented security logging requirements. The Agency logged only basic information about potential security breaches and not advanced information as required, such as user behavior monitoring to detect improper access and compromised systems. The Agency also has not implemented a related prior recommendation.

IAF lacked complete information for its software and hardware inventory. This increases the risk that it will misallocate resources for unneeded software and hardware and reduces its ability to implement effective security controls.

IAF did not conduct annual security control assessments or identify required controls for selected systems. This increases the Agency's risk of exposure to cybersecurity threats and means that leadership cannot have assurance that all controls are operating as intended.

IAF did not consistently develop and maintain security plans for selected systems. Incomplete plans may lead to misinformed decisions on mitigating risk and increase risks of unauthorized access, disruption, and modification of systems.

Introduction

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agency systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) requires our office to conduct an annual independent assessment of the Inter-American Foundation's (IAF) information security programs and practices and report the results of the assessments to the Office of Management and Budget (OMB).

We conducted this evaluation to determine whether IAF implemented an effective information security program.[1] We focused on IAF's information security program for fiscal year (FY) 2025 as of June 20, 2025. We selected this timeframe to ensure that we could provide the results of our assessment of the FY 2025 FISMA reporting metrics by August 1, 2025, as OMB required.

To answer the objective, we followed OMB and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) FY 2025 FISMA reporting metrics and *FISMA Evaluator's Guide*. Ultimately, we could not complete all the procedures needed to answer our objective because most IAF staff were placed on administrative leave during our fieldwork and could not provide the documentation we needed to complete our evaluation.[2] Though one key official became available at the end of fieldwork, due to limited staffing, he was unable to provide enough information for us to complete our assessment.

Despite this limitation, we were able to perform certain procedures and assess certain elements of IAF's information security program. We reviewed the Agency's policies, procedures, and plans to gain an understanding of its information security program. To the extent possible, we analyzed the effectiveness of IAF's information security program by reviewing system user listings, systems security plans, risk assessment reports, vulnerability scan results, and system logs, among other things. For this evaluation, we judgmentally selected four of six systems in IAF's inventory as of October 15, 2024. We selected one system because it was IAF's only internal system and provided general support to other Agency systems and would put those systems at risk if it was not secure. We selected three external systems on an annual rotation plan to ensure that we evaluated every system that would have a moderate effect on the Agency if it were breached.[3]

[1] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 IG FISMA reporting metrics.
[2] Executive Order 14217, "Commencing the Reduction of the Federal Bureaucracy," February 19, 2025, required IAF to "reduce the performance of [its] statutory functions and associated personnel to the minimum presence and function required by law." In the following months, IAF's staffing was significantly reduced.
[3] NIST, *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standards Publication 199), February 2004, defines a moderate effect as "the loss of confidentiality, integrity, or availability [that] could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."

We conducted our work from September 2024 to January 2026 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Appendix A provides more detail on our scope and methodology.

Background

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 requires agency heads to implement policies and procedures to protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

OMB and CIGIE provide instructions on assessing the effectiveness of agency information security programs. To help facilitate these assessments, the instructions contain metrics that inspectors general (IGs) must evaluate for FY 2025.[4]

Various requirements are in place to help IAF implement an effective information security program. For example, OMB Memorandum M-21-31 requires agencies to share information to accelerate responses to information security incidents.[5] It standardizes requirements for logging, retaining, and managing incidents across the government. The National Institute of Standards and Technology (NIST) provides a set of security and privacy controls that agencies can use to protect their information systems and data.[6] It establishes requirements for developing and documenting an accurate inventory of information system components to ensure effective security, configuration management and risk management. It also describes the required contents for a system security plan, providing a clear framework for managing system security risk. Finally, it outlines requirements for system security assessments, which are key for determining the effectiveness of controls, identifying weaknesses, and supporting risk management decisions.

In addition, IAF's procedures provide guidance on the protection of the Agency's information system assets, including instructions on remediating identified system vulnerabilities, which help secure its network.[7] IAF's chief information security officer is responsible for securing the Agency's systems and ensuring that all security requirements are implemented Agency-wide.

In our FY 2024 FISMA audit, our contracted audit firm concluded that IAF implemented an effective information security program.[8] However, the firm found that IAF did not timely mitigate vulnerabilities on one system, update the security plan for one system, or meet

[4] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (version 2.0), April 3, 2025.
[5] OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, (M-21-31) August 27, 2021.
[6] NIST, Special Publication (SP) 800-53 rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020.
[7] IAF, *Information System Security Standard Operating Procedure*, March 2024.
[8] USAID OIG, *FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended* (A-IAF-24-002-C), August 23, 2024.

requirements for logging information security events. To address the weaknesses, the firm made two recommendations in addition to referencing one prior open recommendation. In addition, one recommendation from our FY 2023 FISMA audit was still open.[9] Appendix B provides details on the status of our prior recommendations.

OIG Could Not Determine the Overall Effectiveness of IAF's Information Security Program but Did Identify Weaknesses

We could not determine the overall effectiveness of IAF's information security program for FY 2025 due to access limitations. Most of the Agency's staff was placed on administrative leave for a portion of the evaluation period, preventing us from obtaining necessary information. Despite this, we determined that the Agency met requirements for certain areas and implemented two of four prior FISMA recommendations. However, IAF did not remediate critical vulnerabilities, fully meet security logging requirements, or implement two related recommendations. IAF also did not maintain complete information for its software and hardware inventory, perform security control assessments or identify the controls it assessed for selected systems, or develop and maintain a complete security plan for selected systems.

OIG Could Not Determine the Overall Effectiveness of IAF's Security Information Program in FY 2025

Due to our limited access to Agency staff and essential documents, we did not obtain sufficient, appropriate evidence to fully assess or reach a conclusion on the overall effectiveness of IAF's information security program in FY 2025.

However, based on our analysis of information we did obtain, we found that certain areas met NIST requirements. For example, IAF:

- Developed and maintained its supply chain policies and procedures and monitored suppliers.[10]
- Established requirements for monitoring security incidents, including detection, analysis, and handling.[11]
- Tested its contingency plans to determine whether it could restore normal operations after a security incident.[12]

[9] The contracted audit firm for our FY 2024 FISMA audit did not include this recommendation in the report because it was outside the scope of the review.
[10] NIST SP-800 53 rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, SA-4, Acquisition Process, SA-9 External System Services.
[11] NIST SP-800 53 rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, IR-4, Incident Handling.
[12] NIST SP-800 53 rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, CP-4, Contingency Plan Testing.

IAF Has Continued Challenges in Timely Remediating Critical Vulnerabilities

IAF continued to have issues with remediating critical network vulnerabilities within the timeframes defined by its standard operating procedure (SOP).[13] Specifically, we found that the Agency did not remediate 140 of 947 (14 percent) of the critical vulnerabilities identified in its December 2024 scan report within 15 days, as required. If IAF does not meet the 15-day timeline, it is required to create a plan of action and milestones for remediating overdue vulnerabilities.

We previously recommended that IAF develop and implement a plan to remediate critical vulnerabilities within the timeframe specified in its standard operating procedure to avoid risk of exploitation by attackers.[14] IAF officials said they had taken steps to remediate other vulnerabilities in response to our prior recommendation. In addition, they said they were tracking vulnerabilities on electronic dashboards. However, given the number of vulnerabilities we identified in this evaluation, we found these actions to be insufficient, and the recommendation remains open.

Remediating vulnerabilities, such as applying changes to software to correct security problems, is a key control to reduce the risk that hackers will exploit them by executing malicious code, stealing data, or compromising staff's ability to access systems.[15] Addressing our prior recommendation would better position IAF to remediate critical vulnerabilities in its network in a timely manner.

IAF Has Not Fully Implemented Security Logging Requirements

IAF continues to not meet OMB's logging requirements for potential IT security breaches. OMB defines tiers of information to log for security events: basic, intermediate, and advanced.[16] Since August 2023, our reviews have found that IAF logged only basic information about potential security breaches, such as a timestamp (time, date, and location of incident), serial number, and username (unique logger identifier), when appropriate.[17] However, IAF did not monitor or log advanced information as required, such as user behavior monitoring to detect

[13] IAF, *Information System Security Standard Operating Procedure*, March 2024. Critical vulnerabilities are the most severe security weaknesses in software, hardware, or systems. These vulnerabilities are highly exploitable, can lead to severe consequences, and affect large number of users or systems.
[14] Recommendation 1 in USAID OIG, *FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended* (A-IAF-24-002-C), August 23, 2024.
[15] NIST SP 800-40 rev. 4, *Guide to Enterprise Patch Management Planning,* April 2022, explains that "once a new vulnerability becomes publicly known, risk usually increases because attackers are more likely to develop exploits that target the vulnerable software."
[16] OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, (M-21-31) August 27, 2021. Agencies were to implement: (1) basic level logging requirements by August 2022, (2) intermediate level logging requirements by February 2023, and (3) advanced level logging requirements by August 2023.
[17] Recommendation 3 in USAID OIG, *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-IAF-23-001-C), August 28, 2023.

improper access and compromised systems, which is essential for early detection of malicious behavior.

In July 2024, IAF officials said that they would implement advanced-level logging requirements in response to our recommendation.[18] However, as of July 2025, IAF was still logging only basic information. IAF officials told us they were unable to meet the logging requirements due to funding constraints and noted that agencies of the same size were having similar challenges. Specifically, they noted that the cost of advanced-level logging was significant and that they had prioritized other critical funding needs. However, the officials said they were researching more cost-effective solutions to meet the requirement.

By not meeting these requirements in a timely manner, IAF continues to limit its ability to rapidly respond to security incidents and hampers its efforts to effectively defend its systems and information. As such, we consider our prior recommendation open and still relevant.

IAF Lacked Complete Information for Its Software and Hardware Inventory

IAF did not fully maintain and update its inventory of software and hardware assets as NIST requires.[19] For example, none of the 1,663 software programs listed in the Agency's inventory included the original manufacturer name, version number, or serial number, which is needed to identify specific programs.[20]

For effective management of software and hardware, NIST states that organizations should develop and document an inventory of system components that accurately reflects the system, includes all system components, and is at the level of granularity deemed necessary for tracking and reporting.[21] Additionally, IAF's SOPs state that the Agency must maintain an inventory of its software and hardware assets within its authorization boundary and review the inventory at least annually. [22] Further, the inventory must include the system/component owner, manufacturer name, version number, and serial number.[23]

We determined that IAF lacked crucial and required software and hardware inventory information for several reasons. First, IAF did not conduct an annual review of the inventory in FY 2025, as its SOP requires. Instead, IAF planned to review and update its inventory in the first quarter of calendar year 2026. IAF officials stated that their master inventory was "a living document under continuous review." Our evaluation found that IAF only updated the inventory

[18] USAID OIG, *FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended* (A-IAF-24-002-C), August 23, 2024.
[19] NIST SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems,* September 2020, CM-8 "System Component Inventory."
[20] Version numbers are used in software inventory management as a unique identifier. The version number indicates the changes made to the software overtime, including security improvements.
[21] NIST SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems,* September 2020, CM-8 "System Component Inventory."
[22] NIST defines an authorization boundary as the components of an information system that are approved for operation.
[23] IAF *Information System Security Standard Operating Procedure,* March 2024.

to reflect certain changes, such as returns and assignments of laptops. Agency staff did not review the entire inventory for accuracy and completeness, as required.

Second, the SOP did not require the inventory to include the necessary information NIST requires, such as device type, location, and software license information. IAF officials stated that the SOP did not require this information because the inventory listing was structured to collect essential elements needed to track Agency assets, and the information was not considered essential. However, we concluded that IAF's inventory lacks necessary information for assuring its completeness and accuracy. For example, officials cannot determine whether hardware assets are missing because the inventory does not track location. IAF also cannot determine whether software assets are being used and should be maintained because the inventory does not track licensing information.

Inventory management is a critical control for helping an agency maintain visibility over its digital assets. An inventory that lacks necessary information increases the risk that IAF will misallocate resources for unneeded software and hardware. It can further hinder the Agency's ability to implement effective security controls, such as remediating vulnerabilities, which ultimately undermines its ability to secure its information technology environment.

IAF Did Not Conduct Annual Security Control Assessments or Identify Required Controls for Selected Systems

IAF did not perform security assessments for two of the four selected systems, as required by its policies. Further, although IAF assessed the third system, the security assessment report did not identify which controls were included. IAF was not responsible for conducting security control assessments for the fourth system. According to the Agency's SOP, system owners are required to assess a third of all controls annually and document the results of the assessment for the chief information officer and chief information security officer.[24] Further, NIST requires agencies to describe the controls they assess.[25]

IAF did not perform security assessments for two of the systems because its SOP does not discuss holding system owners accountable for following the procedure. For example, the procedure did not require the chief information security officer to report noncompliance to the system owner's supervisor. Instead of conducting assessments, IAF officials said they reviewed health checks on these two systems. However, a health check shows a high-level snapshot of a system, while a security controls assessment is an in-depth review to determine if security controls are operating effectively.

In addition, IAF did not identify the controls it assessed for the third system because the procedures did not require the Agency to do so. Instead, IAF management said that the Agency

[24] IAF, *Information System Security Program Standard Operating Procedures,* March 2024. A *system owner* is a person or organization with responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. A *chief information officer* is responsible for developing, maintaining, and facilitating the implementation of a sound and integrated information architecture for the agency. A *chief information security officer* is responsible for developing, implementing, and enforcing security policies to protect critical data.

[25] NIST SP 800-53 rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, CA-2, (Control Assessments).

lists the controls assessed in another security document. Our review of that document found that it did not specify the controls assessed or the timing of those assessments.

Security controls assessments help agencies identify weaknesses in a system, thus providing essential information for making risk-based decisions about whether to operate it. The lack of a yearly assessment could lead to unmitigated vulnerabilities, increasing IAF's risk of exposure to cybersecurity threats. In addition, without updates to security assessment reports to specify the assessed controls, Agency leadership cannot have assurance that all controls are operating as intended.

IAF Did Not Consistently Develop and Maintain Security Plans for Selected Systems

We identified weaknesses in IAF's efforts to develop and maintain security plans for the four systems we evaluated. Such plans are required and essential to define the security controls in place to protect an information system. For two of the systems we evaluated, the security plans included only the security controls but lacked other essential elements NIST requires. This included types of information processed, stored, and transmitted by the system; roles and responsibilities of users; and a clear description of current security controls and the plans for putting them in place.[26] For the third system, IAF did not review and update its system security plan every 3 years; the plan was last updated in 2021. For the fourth system, IAF never developed a system security plan.

In addition to the NIST requirements, IAF's SOP directs the authorizing official to review and update the system security plan every 3 years or when there are significant changes to the system.[27]

For the two systems with security plans, IAF did not include the essential elements because it did not have a procedure to hold system owners accountable for completing the plans, as required. IAF officials stated that they documented the required elements of the security plan in risk assessment reports because they believed that was sufficient for making a risk-based decision. However, a risk assessment considers threats, vulnerabilities, likelihood, and impact to organizational vulnerabilities in the system. It does not include key elements, such as types of information processed, stored, and transmitted by system; roles and responsibilities of users; and a clear description of current security controls and the plans for putting them in place. This information is important for providing a clear understanding of what information needs to be protected within a system, assessing risk, and identifying controls to secure a system.

For the system with the outdated security plan, IAF officials stated that they did not update it within 3 years because they were making major changes to their network. However, this does not justify the outdated plan. We previously reported that IAF was finalizing an updated security plan to incorporate NIST requirements in response to our FY 2024 recommendation.[28]

[26] NIST SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020, PL-2, System Security and Privacy Plans.
[27] IAF, *Information System Security Program Standard Operating Procedures,* March 2024.
[28] USAID OIG, *FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended* (A-IAF-24-002-C), August 23, 2024.

After we completed fieldwork for this evaluation, IAF provided us with an updated system security plan to close the prior audit recommendation. After reviewing the plan, we agreed that the Agency had taken corrective action and closed the recommendation. Therefore, we are not making a new recommendation.

For the fourth system, IAF did not develop a security plan because Agency officials accepted the risk of relying on a third-party entity. However, risk acceptance does not replace the requirement for an agency-specific system security plan. IAF officials acknowledged that they were responsible for certain controls. However, although we requested it, they did not provide a document, such as a customer responsibility matrix, that identified the controls and did not prepare a plan for implementing them.[29]

System security plans are important because they describe the security controls in place and the plan and status for meeting the control requirements. An incomplete plan undermines the system's security posture, which may lead to misinformed decisions on mitigating risk. IAF cannot have assurance that it has implemented all the controls necessary to protect the network unless it maintains an up-to-date system security plan. The lack of an understanding of responsibilities for controls also increases the risk of security control gaps. As a result, IAF risks unauthorized access, disruption, and modification to the systems and destruction and disclosure of the information they contain.

Conclusion

We could not determine whether IAF implemented an effective information security program in FY 2025 due to the unavailability of Agency officials. Though one key official became available at the end of fieldwork, due to limited staffing, he was unable to provide enough information for us to complete our assessment. Nonetheless, we identified weaknesses that warrant IAF's attention to ensure that the Agency has a robust information security program that mitigates risks to systems and sensitive information. Taking action to remediate longstanding critical vulnerabilities and logging security events is crucial for protecting the Agency's information and systems, as is assessing security controls, developing a comprehensive inventory, and completing security plans. By taking steps to address identified weaknesses, IAF will better protect its information systems from cyberattacks and other security challenges, ultimately reducing the opportunity for bad actors to access government resources and sensitive operating data.

[29] A customer responsibility matrix identifies security controls that a cloud service provider is responsible for implementing and the customer is responsible for implementing.

Recommendations

We recommend that IAF's Chief Information Security Officer take the following actions:

1. Conduct a comprehensive review of IAF's software and hardware inventories and update them to ensure that they are accurate and complete.
2. Update IAF's procedures to include all elements for tracking the Agency's software and hardware assets. At a minimum these elements should include device type, location, and software license information.
3. Conduct a security controls assessment for the two systems identified.
4. Develop and implement procedures to hold system owners accountable for conducting security controls assessments and completing system security plans, and document which security controls are assessed and when.
5. Update security plans for the two systems identified to include all required components as outlined in NIST Special Publication 800-53.
6. Document the controls IAF is responsible for implementing for the external system identified and develop and implement a security plan for the system.

OIG Response to Agency Comments

We provided our draft report to IAF on January 22, 2026. On February 10, 2026, we received the Agency's response, which is included in Appendix C of this report.

The report included six recommendations. We acknowledge management decisions on the recommendations and consider them resolved but open pending completion of planned activities.

Appendix A. Scope and Methodology

We conducted our work from September 2024 to January 2026 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Our objective was to determine whether IAF implemented an effective information security program.[30]

Our review focused on IAF's information security program for FY 2025 through June 20, 2025. We selected this timeframe to ensure that we could provide the results of our assessment of the FY 2025 FISMA reporting metrics to the Agency by August 1, 2025, as OMB required. In one instance, we received and reviewed IAF's supporting documentation for a prior recommendation after June 20, 2025. We engaged with staff at IAF's headquarters in Washington, DC, when possible.

After February 19, 2025, nearly all IAF's personnel were placed on administrative leave. This action occurred during our fieldwork, which meant we were unable to obtain sufficient and appropriate evidence to fully verify certain required FY 2025 IG metrics. Though one key official became available at the end of fieldwork, due to limited staffing, he was unable to provide enough information for us to complete our assessment.

To answer our objective, we followed the FY 2025 IG FISMA reporting metrics and IG *FISMA Evaluator's Guide*, which provides a baseline of suggested evidence and test steps for FISMA-related evaluations.[31] We used criteria referenced throughout the metrics to assess the effectiveness of IAF's information security controls, including NIST Special Publication 800-53, rev. 5, NIST Cybersecurity Framework, and OMB circulars. In addition, we used IAF's IT System Security SOP to assess the effectiveness of the controls.

We judgmentally selected four of six systems in IAF's inventory as of October 15, 2024, for certain tests. We selected one system because it was IAF's only internal system, provided general support to other Agency systems, and would put those other systems at risk if it was not secure. We selected the three external systems on an annual rotation plan to ensure that we evaluated every system that would have a moderate effect on the Agency if breached.[32]

Ultimately, we could not complete all the procedures needed to answer our objective. After February 19, 2025, nearly all IAF's personnel were placed on administrative leave.[33] Because this occurred during our fieldwork, we could not obtain sufficient and appropriate evidence to

[30] For this evaluation, we defined an effective information security program as one that has an overall mature program based on the FY 2025 FISMA reporting metrics.
[31] CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, version 1.0, May 5, 2025.
[32] NIST, *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standards Publication 199), February 2004, defines a moderate effect as "the loss of confidentiality, integrity, or availability [that] could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."
[33] Executive Order 14217, "Commencing the Reduction of the Federal Bureaucracy," February 19, 2025, required IAF to "reduce the performance of [its] statutory functions and associated personnel to the minimum presence and function required by law." In the following months, IAF's staffing was significantly reduced.

assess certain control areas or fully verify certain required FY 2025 IG metrics. Specifically, IAF did not provide:

- Policies for developing and maintaining its inventory of data and metadata.
- Documents showing that it has implemented processes for managing privileged accounts.
- Policies for monitoring and measuring the integrity and security posture of all owned and associated assets.

Nonetheless, we were able to perform certain tests. For example, we reviewed IAF's:

- Information security program SOP dated March 2024 to determine whether IAF defined its risk management processes in accordance with NIST guidance.
- Processes for identifying supply chain requirements and vendor supplier reports to determine whether the supply chain requirements complied with NIST guidance.
- Asset inventory listing and related policies and procedures to understand the Agency's inventory management process and determine whether IAF tracked and classified its assets, as NIST requires.[34]
- Information System Security SOP, dated March 2024, to understand the Agency's vulnerability management process. We also reviewed its vulnerability scanning report dated December 2, 2024, and patch management report dated December 10, 2024, to determine whether vulnerabilities were remediated and patched within the organization's defined timeframes.
- Continuous monitoring policies and procedures and security assessment documentation to determine IAF's process for conducting security assessments. We further selected four systems and reviewed security documents, such as the authorization to operate, system security plan, and security assessment report, to determine whether IAF conducted and documented assessments in accordance with NIST guidelines.
- Policies and procedures on incident response to determine whether the Agency developed and implemented processes around incident detection and analysis, in accordance with NIST SP 800-53 rev 5.
- Policies and procedures on contingency planning and contingency plan test results and reports to determine whether IAF conducted contingency-related actions in accordance with NIST SP 800-53 rev 5.

To determine the status of recommendations we made to IAF in our FY 2023 and FY 2024 FISMA audit reports, we reviewed the Agency's closure requests and supporting documentation. Appendix B provides details on these recommendations.

[34] NIST SP 800-53 rev. 5, *Security and Privacy Controls for Information Systems,* September 2020, CM-8 (System Component Inventory).

Appendix B. Status of Prior Recommendations

This table provides the status of recommendations from our FY 2023 and FY 2024 FISMA audit reports that were open as of October 1, 2024, the beginning of the period covered by our evaluation.[35]

Table 1. Prior OIG Recommendations

Report & Recommendation #	Recommendation	IAF's Position	Evaluator's Position
A-IAF-23-001-C (FY 2023 Rec.2)	We recommend that IAF's Chief Information Officer develop and implement procedures for compensating controls in lieu of multifactor authentication for systems that the agency plans to decommission.	Closed	Closed
A-IAF-23-001-C (FY 2023, Rec. 3)	We recommend that IAF's Chief Information Officer implement level 2 event logging requirements in accordance with Office of Management and Budget Memorandum, M-21-31.	Open	Open
A-IAF-24-002-C (FY 2024, Rec. 1)	We recommend that IAF's Chief Information Officer develop and implement a plan, including tools and other resources, to remediate critical and high vulnerabilities within the timeframes specified in the agency's Information System Security Program Standard Operating Procedures (February 2022).	Open	Open
A-IAF-24-002-C (FY 2024, Rec. 2)	We recommend that IAF's Chief Information Officer update its system security plan to include controls in National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."	Closed	Closed

Source: OIG's FY 2023 and 2024 FISMA audit reports and assessment of IAF's recommendation closure requests and supporting documentation.

[35] USAID OIG, *IAF Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-IAF-23-001-C), August 28, 2023, and USAID OIG, *FISMA: IAF's Information Security Program for Fiscal Year 2024 Was Effective, Although Improvements Are Recommended* (A-IAF-24-002-C), August 23, 2024.

Appendix C: Agency Comments

INTER-AMERICAN FOUNDATION
EMPOWERED COMMUNITIES, SUSTAINABLE RESULTS

February 10, 2026

Ms. Gabriele Tonsil
Acting Assistant Inspector General for Audits, Inspections, and Evaluations
Office of Inspector General
U.S. Agency for International Development

Dear Ms. Tonsil,

I write to provide the Inter-American Foundation (IAF)'s management comments and actions undertaken or planned to address the recommendations contained in the evaluation of IAF's information security program for FY 2025.

The IAF recorded no security incidents in 2025 and continues to maintain a serious, disciplined, and iterative approach to continuous improvement across our cybersecurity and enterprise risk programs. Although we recognize that there is always room for improvement, we are confident that our information security program was and is effective.

The FY 2025 evaluation took place during a year of turbulence and extenuating circumstances. IAF staff members worked diligently through the changes to address risks and strengthen our information security program. The IAF moved offices in December 2024 and simultaneously transitioned equipment, including a significant upgrade to the efficiency and maturity of our servers via transitioning to the cloud. Staff returned to full-time in-office work in March 2025, again requiring IT infrastructure adjustment. Shortly thereafter, the IAF experienced a period where contracts were cancelled and most staff were placed on administrative leave before being reinstated in April 2025.

During the evaluation review period, the Office of the Inspector General transitioned from a contractor-led to an in-house-led evaluation and the IAF adjusted to provide information to both parties. Transitions at both agencies thus increased the challenges of completing a comprehensive review and the timelines to resolve recommendations.

We appreciate the recommendations and your team's cooperation with IAF staff as we continue working to address them, as described below.

1331 Pennsylvania Ave., N.W. | Suite 300 South | Washington, D.C. 20004 | www.iaf.gov

The FY 2025 evaluation identified six new recommendations and two recommendations carried over from FY 2024. The IAF recognizes these are areas for improvement and has closed one recommendation and has already completed initial phases of addressing the remaining recommendations. The IAF targets full completion of the remaining new recommendations by September 30, 2026.

Recommendation 1: *Conduct a comprehensive review of IAF's software and hardware inventories and update them to ensure that they are accurate and complete.*

Recommendation 2: *Update IAF's procedures to include all elements for tracking the Agency's software and hardware assets. At a minimum these elements should include device type, location, and software license information.*

IAF Responses 1 & 2: *Partially resolved, full completion by September 30, 2026.* The IAF's hardware inventory was reviewed and is now accurate and complete, with the required data elements where applicable. The IAF's current software inventory will be updated to include the additional requirements in FY 2026. The IAF is reviewing appropriate software tracking practices and tools and will update the procedures for asset tracking in FY 2026.

Recommendation 3: *Conduct a security controls assessment for the two systems identified.*

Recommendation 4: *Develop and implement procedures to hold system owners accountable for conducting security controls assessments and completing system security plans, and document which security controls are assessed and when.*

Recommendation 5: *Update security plans for the two systems identified to include all required components as outlined in NIST Special Publication 800-53.*

IAF Responses 3, 4, & 5: *Full completion by September 30, 2026.* The IAF takes security control assessments seriously and has prioritized doing health checks on the systems to make sure that the agency understands any risks posed by the system. The agency will update its procedures and conduct a full security controls assessment for the two systems and has already dedicated resources to do so in FY 2026. A contractor has been hired to support the security assessment process and will support updating the procedures and conducting security control assessments. The security plans for the two systems will be updated to include the additional data fields in FY 2026 with the support of the contractor.

Recommendation 6: *Document the controls IAF is responsible for implementing for the external system identified and develop and implement a security plan for the system.*

IAF Response 6: *Full completion by September 30, 2026.*

IAF operates this system under an Authority to Use (ATU) which specifically adopts the security plan (SSP) and customer risk matrix (CRM) from the Authority to Operate (ATO) provided by an authorizing provider. NIST SP 800-7, Rev. 2, Appendix F permits an agency to use an Authorization to Use (ATU) "when an organization chooses to accept the information in an existing authorization package produced by another organization for an information system that is authorized to operate by a federal entity" (parentheticals removed). The SSP and CRM are both a part of the existing authorization package and were reviewed by the IAF in issuing an ATU. Therefore in granting an ATU for Google Workspace, a FedRAMP-authorized system, the IAF also gained the efficiencies of adopting the SSP and CRM in the authorization package and is not required to develop or implement another such plan. IAF's ATU already explicitly accepts the SSP from the authorization package. The IAF will update its ATU to specifically reference acceptance of the CRM and will document how it is implementing the customer organization controls in the CRM in FY 2026.

In addition to the new recommendations, the IAF continues to work on two recommendations from FY 2024.

2024 Recommendation 1: *IAF Needs to Remediate Critical and High Vulnerabilities Within Its Defined Remediation Timeframe. We recommend that IAF's Chief Information Officer develop and implement a plan, including tools and other resources, to remediate critical and high vulnerabilities within the timeframes specified in the agency's Information System Security Program Standard Operating Procedures (February 2022).*

IAF Response 2024-1: *Updated timeline, full completion by September 30, 2026.* IAF has made significant progress on the metrics used in measuring compliance through a transition to an automated tracking and prioritization system that continuously monitors IAF assets to ensure timely remediation; however, the agency's SOP has not yet been updated to reflect the improved process. The IAF has therefore largely mitigated the risk, but recognizes the need to conform the SOP to the new process. The IAF will update its SOP in FY 2026 to reflect the remediation procedures.

2024 Recommendation 3: IAF Needs to Implement Event Logging Requirements Set Forth by OMB M-21-31.

IAF Response 2024-3: The IAF acknowledges that it currently meets Event Logging Level 1 (EL1) standards and has not yet fully implemented the Level 2 (EL2) or Level 3 (EL3). However,

this is due to the high cost of available solutions and the IAF has been forced to accept the risk of remaining at EL1 until an affordable solution is found. The agency has been and continues to actively research cost-effective, cloud-native solutions that may allow for incremental improvements in logging maturity and welcomes any solutions that OIG can share for similarly-sized agencies. IAF IT staff members have reached out to other micro agencies for workable solutions and have been informed that it is a common struggle.

Thank you and your team for continuing to provide important feedback on the IAF's operations. As a federal agency, we take great pride in our work and recognize the responsibility of good stewardship and continuous improvement that comes with that position.

Sincerely,

/s/

Sara Aviel
President & CEO

Visit our website at oig.usaid.gov and
follow us on social media.

X: @AidOversight
LinkedIn: USAID Office of Inspector General
Instagram: @usaid.oig

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

Report Waste, Fraud, and Abuse
Online Complaint Form