
OFFICE OF INSPECTOR GENERAL

# 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

WASHINGTON, DC

*Office of Inspector General*

November 7, 2016

Rajiv Jain, Chief Information Officer
Inter-American Foundation
1331 Pennsylvania Avenue NW
Suite 1200 North
Washington, DC 20004

Dear Mr. Jain:

Enclosed is the final report, "The Inter-American Foundation Has Implemented Many Controls in Support of FISMA, but Improvements Are Needed" (A-IAF-17-004-C). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. According to Clifton officials, this audit was performed in accordance with generally accepted government auditing standards.

In carrying out our oversight responsibilities, we reviewed the report and related audit documentation to determine whether Clifton complied with U.S. generally accepted government auditing standards. Our review was different from an audit in accordance with those standards and was not intended to enable us to express, and we do not express, an opinion on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We did not find any instances of Clifton not complying, in all material respects, with applicable standards.

The audit objective was to determine whether IAF implemented security controls for selected information systems in support of FISMA. (Appendix III lists controls and systems selected and rates their effectiveness.) To answer the audit objective, Clifton tested IAF's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." The audit included two IAF-managed information systems—the Enterprise Network and the Grants Evaluation and Management System—and one contractor system, Google Mail. Clifton conducted fieldwork at IAF's headquarters in Washington, DC, from April 6 through August 5, 2016.

The audit concluded that IAF generally complied with FISMA requirements by implementing 84 of 98 security controls for selected information systems. However, IAF did not implement 14 controls designed to preserve the confidentiality, integrity, and availability of its information and information systems.

IAF complied with many FISMA requirements, including the following:

- Maintaining effective change management policy and procedures.
- Implementing effective security awareness and training procedures.

- Maintaining adequate incident response and reporting policy and procedures.
- Maintaining adequate procedures for bringing on new employees and ensuring terminated employees' access was removed promptly.

However, IAF still needs to do the following:

- Mitigate network vulnerabilities (1 control weakness).
- Implement a continuous monitoring program (1 control weakness).
- Strengthen baseline configuration monitoring (1 control weakness).
- Strengthen the security assessment and authorization process and assess system risks (1 control weakness).
- Implement audit log and monitoring controls (1 control weakness).
- Implement multifactor authentication for the Enterprise Network (1 control weakness).
- Update and test the continuity of operations plan (2 control weaknesses).
- Strengthen the process to validate whether plans of action and milestones are complete and up to date (1 control weakness).
- Update information system standard operating procedures to include privacy controls (1 control weakness).
- Update the Enterprise Network system security plan to reflect the current operating environment (1 control weakness).
- Implement information system agreements for all external systems (1 control weakness).
- Document an information system inventory to include internal and external systems (1 control weakness).
- Strengthen account management controls for the Grants Evaluation and Management System (1 control weakness).

To address the weaknesses identified in Clifton's report, OIG makes the following recommendations to IAF's management.

***Recommendation 1.*** *We recommend that the Inter-American Foundation's chief information officer remediate vulnerabilities in the network identified by the Office of Inspector General's contractor and document the results or document acceptance of the risks of those vulnerabilities.*

***Recommendation 2.*** *We recommend that the Inter-American Foundation's chief information officer develop and implement a continuous monitoring plan and program.*

***Recommendation 3.*** *We recommend that the Inter-American Foundation's chief information officer develop and implement monitoring controls of baseline configurations for the Enterprise Network and document the results.*

***Recommendation 4.*** *We recommend that the Inter-American Foundation's chief information officer complete a system risk assessment for the Enterprise Network that takes into account all known vulnerabilities, threat sources, and security controls planned or in place, determine the residual risk, and inform the authorizing official of the security state of the information system.*

***Recommendation 5.*** *We recommend that the Inter-American Foundation's chief information officer obtain a current authorization to operate the Enterprise Network that*

*results from a completed security controls assessment and updated system security plan, risk assessment, and plan of action and milestones.*

***Recommendation 6.*** *We recommend that the Inter-American Foundation's chief information officer document and implement a process to review and analyze auditable events.*

***Recommendation 7.*** *We recommend that the Inter-American Foundation's chief information officer implement multifactor authentication for all network accounts and document the results.*

***Recommendation 8.*** *We recommend that the Inter-American Foundation's chief information officer update the continuity of operations plan to include a business impact analysis.*

***Recommendation 9.*** *We recommend that the Inter-American Foundation's chief information officer document and implement a process to validate annual testing of the continuity of operations plan.*

***Recommendation 10.*** *We recommend that the Inter-American Foundation's chief information officer develop and implement a written process to validate whether the plan of action and milestones is completed and updated promptly and includes all applicable control weaknesses.*

***Recommendation 11.*** *We recommend that the Inter-American Foundation's chief information officer update and implement the Information System Security Program Standard Operating Procedures to include the privacy controls identified in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."*

***Recommendation 12.*** *We recommend that the Inter-American Foundation's chief information officer update the organization's Enterprise Network and Software Applications System Security Plan to reflect the current operating environment.*

***Recommendation 13.*** *We recommend that the Inter-American Foundation chief information officer obtain a written, fully executed Interconnection Security Agreement with the Department of Interior Business Center.*

In finalizing the report, Clifton evaluated IAF's responses on the 13 recommendations. Based on those responses, we acknowledged management decisions on recommendations 1 through 13. For recommendation 6, we disagree that final action has been taken. Further, we acknowledge final action has been taken on recommendation 13.

We appreciate the cooperation and courtesies extended to our staff and Clifton's employees during the audit.

Sincerely,

/s/

Alvin A. Brown
Deputy Assistant Inspector General for Audit

cc: Robert N. Kaplan, President and Chief Executive Officer, IAF
Lesley Duncan, Chief Operating Officer, IAF

CliftonLarsonAllen LLP
4250 N. Fairfax Drive, Suite 1020
Arlington, Virginia 22203
571-227-9500 fax 571-227-9552
www.claconnect.com

October 31, 2016

Mr. Mark Norman
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 Mr. Norman:

Enclosed is the final version of our report on the Inter-American Foundation's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The Inter-American Foundation Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed*. The USAID Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the audit in support of the FISMA requirement for an annual evaluation of IAF's information security program.

The objective of this performance audit was to determine whether IAF implemented selected security controls for selected information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

For this audit we reviewed two IAF-managed information systems, the Enterprise Network and the Grants Evaluation and Management System, and one contractor system, Google Mail. The Enterprise Network provides the infrastructure that supports mission-critical and mission-important applications as well as administrative and minor applications. GEMS tracks all grant activity for IAF. Audit fieldwork was performed at the Inter-American Foundation's headquarters in Washington, D.C., from April 6, 2016, to August 5, 2016.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit concluded that IAF generally complied with FISMA requirements by implementing 84 of 98 selected security controls for selected information systems. Although IAF generally had policies for its information security program, its implementation of those policies for 14 of the 98 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently,

the audit identified areas in IAF's information security program that needed to be improved. We are making thirteen recommendations to assist IAF in strengthening its information security program.

In response to the draft report, IAF outlined and described its plans to address all thirteen audit recommendations. Based on our evaluation of management comments, we acknowledge management decisions on all 13 recommendations, though we disagree that final action has been taken on recommendation 6. Further, we acknowledge final action has been taken on recommendation 13. IAF's comments are included in their entirety in Appendix II.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of IAF and appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

*4250 N. Fairfax Drive*
*Suite 1020*
*Arlington, Virginia 22203*
tel: 571-227-9500
fax: 571-227-9552

**www.claconnect.com**

# The Inter-American Foundation Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed

## Fiscal Year 2016

## Final Report

*4250 N. Fairfax Drive*
*Suite 1020*
*Arlington, Virginia 22203*
tel: 571-227-9500
fax: 571-227-9552

**www.claconnect.com**

# TABLE OF CONTENTS

# SUMMARY OF RESULTS

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires 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 source. Because the Inter-American Foundation (IAF) is a federal agency, it is required to comply with federal information security requirements.

The act also requires agency heads to ensure that (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. All agencies must also report annually to the Office of Management and Budget and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology are mandatory for Federal agencies.

The USAID Office of Inspector General engaged us, CliftonLarsonAllen LLP (CLA), to conduct an audit in support of the FISMA requirement for an annual evaluation of IAF's information security program. The objective of this performance audit was to determine whether IAF implemented selected security controls for selected information systems[2] in support of FISMA.

Our audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this audit we reviewed two IAF-managed information systems, the Enterprise Network and the Grants Evaluation and Management System, and one contractor system, Google Mail. The Enterprise Network provides the infrastructure that supports mission-critical and mission-important applications as well as administrative and minor applications. GEMS tracks all grant activity for IAF.

**Results**

The audit concluded that IAF generally complied with FISMA requirements by implementing 84 of 98 selected security controls[3] for selected information systems. For example, IAF complied with the following requirements:

[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] See Appendix III for a list of controls and systems selected.

[3] See Appendix III – Summary of Results of Each Control Reviewed.

- Maintained effective change management policy and procedures.
- Implemented effective security awareness and training procedures.
- Maintained adequate incident response and reporting policy and procedures.
- Maintained adequate processing procedures for bringing on new employees and ensuring terminated employee access was removed timely.

Although IAF generally had policies for its information security program, its implementation of those policies for 14 of the 98 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the foundation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in IAF's information security program that needed to be improved. Specifically, IAF needs to:

- Mitigate network vulnerabilities.
- Implement a continuous monitoring program.
- Strengthen monitoring of baseline configurations.
- Strengthen the security assessment and authorization process and assess system risks.
- Implement controls surrounding audit log and monitoring.
- Implement multi-factor authentication for the Enterprise Network.
- Update the continuity of operation plan and complete testing of the plan.
- Strengthen the plans of action and milestones process.
- Update information system standard operating procedures to include privacy controls.
- Update the Enterprise Network system security plan to reflect current operating environment.
- Implement information system agreements for all external systems.
- Document an information system inventory to include internal and external systems.
- Strengthen account management controls for the Grants Evaluation and Management System.

This report makes 13 recommendations to assist IAF in strengthening its information security program (pages 4-13).

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

In response to the draft report, IAF outlined and described its plans to address all 13 audit recommendations. Based on our evaluation of management comments, we acknowledge management decisions on all 13 recommendations, though we disagree that final action has been taken on recommendation 6. Further, we acknowledge final action has been taken on recommendation 13. IAF's comments are included in their entirety in Appendix II (pages 17 – 22).

# AUDIT FINDINGS

## 1. Network Vulnerabilities Need to Be Mitigated

The National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control RA-5, states the following regarding vulnerability scanning:

> The organization:
>
> * * *
>
> d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

IAF had a process in place to remediate vulnerabilities within patch cycles. However, independent scans performed using the software tool Nessus noted 16 critical and 35 high risk vulnerabilities related to patch management, configuration management and unsupported software. Many of the patch management vulnerabilities were publicly known before 2015, such as those related to ESXi, Oracle, and Symantec Endpoint Protection Manager. In addition, Microsoft Windows SMB Shares were configured with weaknesses that relate to unprivileged access to shared folders. The unsupported software related to Windows Server 2003 still being used by IAF after official support from Microsoft had stopped.

IAF management indicated that the vulnerabilities existed because some users were traveling abroad and their computers were not receiving the updates. IAF is now taking a more targeted approach at vulnerability remediation and is targeting individual computers to patch.

Unmitigated vulnerabilities on IAF's network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known issues to execute arbitrary code.
- Foundation employees may be unable to access systems.
- Foundation data may be compromised.

As a result of the identified vulnerabilities, we are making the following recommendation:

> ***Recommendation 1:*** *We recommend that the Inter-American Foundation's Chief Information Officer either (1) remediate vulnerabilities in the network identified by the Office of Inspector General's contractor, as appropriate, and document the results or (2) document acceptance of the risks of those vulnerabilities.*

## 2. IAF Needs to Implement a Continuous Monitoring Program

NIST Special Publication 800-53, Revision 4, security control CA-7, states the following regarding continuous monitoring:

> 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;
> c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
> d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
> e. Correlation and analysis of security-related information generated by assessments and monitoring;
> f. Response actions to address results of the analysis of security-related information; and
> g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

IAF did not have a continuous monitoring plan and program in place. Due to changes in contractors, IAF was still in process of setting up a continuous monitoring plan and program. Specifically, the new contractor will provide asset discovery, behavioral monitoring, log monitoring, vulnerability assessments and security information and event management services.

Without a continuous monitoring plan and program in place, IAF management does not have insight into their current operating environment to address known control weaknesses proactively or situational awareness to detect loss of information.

> ***Recommendation 2:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement a continuous monitoring plan and program.*

## 3. IAF Needs to Strengthen the Monitoring of Baseline Configurations

NIST Special Publication 800-53, Revision 4, security control CM-2, states the following regarding baseline configurations:

> The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

IAF had developed and documented a baseline configuration for the Enterprise Network; however, IAF did not have controls in place to monitor compliance with the baseline configurations. Due to the change in contractors, IAF no longer had the capability to monitor baseline configurations. IAF's new contractor, hired in April 2016, was in the process of implementing baseline configuration monitoring; however, it had not been implemented at the time of the audit.

Without monitoring baseline configurations, IAF is at an increased risk of vulnerabilities if a system is not configured to the baseline configuration. As a result, we recommend the following:

> ***Recommendation 3:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement monitoring controls of baseline configurations for the Enterprise Network and document the results.*

## 4. IAF Needs to Strengthen the Security Assessment and Authorization Process and Assess System Risks

NIST Special Publication 800-53, Revision 4, security control CA-6, states the following regarding security authorizations:

> The organization:
>
> * * *
>
> c. Updates the security authorization [*Assignment: organization-defined frequency*].

In addition, NIST Special Publication 800-37, Revision 1, states the following regarding the security authorization package, "Assemble the security authorization package and submit the package to the authorizing official for adjudication. *The security authorization package* contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions."

The Enterprise Network Authorization to Operate (ATO) was signed on April 18, 2016, by the Chief Operations Officer (COO); however, the security assessment re-authorization activities were completed a year prior to the signing of the ATO. Specifically, per NIST Special Publication 800-37, Revision 1, after the completion of the security authorization package, the information system owner submits the final package to the authorizing official for a decision. However, the following assessment documentation was not updated when the new ATO was obtained and were completed a year prior to the signing of the ATO:

- Security Assessment Report, April 2015
- Risk Assessment Report, April 2015

The signing of the ATO package was delayed due to internal management discussion on the appropriate personnel to sign off as the authorizing official. In addition, the risk assessment was delayed due to change in contractor and was scheduled to be performed in April 2017.

Without current risk assessments included in the ATO package, senior level agency officials may not make fully informed decisions regarding risks to the system and its operation. As a result, we recommend the following:

***Recommendation 4:*** *We recommend that the Inter-American Foundation's Chief Information Officer complete a system risk assessment for the Enterprise Network that takes into account all known vulnerabilities, threat sources, and security controls planned or in place, and determine the resulting level of residual risk to ensure the authorizing official has appropriate knowledge of the security state of the information system.*

***Recommendation 5:*** *We recommend that the Inter-American Foundation's Chief Information Officer obtain a current authorization to operate for the Enterprise Network that is based on a completed security controls assessment and updated system security plan, risk assessment and plan of action and milestones.*

## 5. Audit Logging and Monitoring Needs to be Implemented

NIST Special Publication 800-53, Revision 4, security control AU-6, states the following regarding audit logging and monitoring:

> The organization:
>
> a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indicators of [*Assignment: organization-defined inappropriate or unusual activity*]; and
> b. Reports findings to [*Assignment: organization-defined personnel or roles*].
>
> Control Enhancements
>
> 1. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

IAF did not have an automated mechanism to integrate audit review, analysis, and reporting processes. IAF was leveraging software from Tru-shield to monitor event logs and alert IAF of inappropriate or unusual activity. The Tru-shield software was managed by a contractor for IAF until March 2016. IAF's new contractor, hired in April 2016, was in the process of setting up an automated audit log and monitoring tool; however, it had not been implemented at the time of the audit.

Without monitoring audit logs, unauthorized individuals may gain system access and conduct malicious activities without detection. As a result, we recommend the following:

***Recommendation 6:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to review and analyze auditable events.*

## 6. IAF Needs to Implement Multi-factor Authentication for the Enterprise Network

NIST Special Publication 800-53, Revision 4, security control IA-2, states the organization should implement multifactor authentication for network and local access for privileged and non-privileged accounts to gain access to the information system.

In addition, Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and* Contractors (August 27, 2004) require the use of Personal Identification Verification for gaining logical access to federally controlled information systems.

IAF did not implement multifactor authentication for network access for its privileged and non-privileged users. Multifactor authentication was only implemented for remote access. Management indicated that it was not feasible or cost effective to implement multi-factor authentication. However, IAF had purchased equipment capable of accepting Personal Identify Verification cards, so it would be ready to use the cards when they are able to do so.

By not implementing multifactor authentication for network access to IAF's network, IAF increases the risk that unauthorized individuals could gain access to its information system and data. As a result, we recommend the following:

> ***Recommendation 7:*** *We recommend that the Inter-American Foundation's Chief Information Officer implement multifactor authentication for all network accounts and document the results.*

## 7. Continuity of Operations Plan Needs to be Updated and Testing Needs to be Completed

NIST Special Publication 800-53, Revision 4, security control CP-2, states the following regarding contingency planning:

> The organization:
>
> * * *
>
> 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.

In addition, NIST Special Publication 800-53, Revision 4, security control CP-4, states the following regarding contingency plan testing:

> The organization:
>
> a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined

tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan.

The IAF Continuity of Operations Plan (COOP) dated April 2015, was not fully completed to include all required elements. Specifically, The COOP did not include a business impact analysis. In addition, the COOP plan did not include recovery time objectives and did not address maintaining business functions, which would be addressed in the business impact analysis. Additionally, IAF did not perform a COOP test for Fiscal Year 2016. IAF was only able to complete a table top exercise, but was not able to perform a full contingency plan test to validate system recovery capabilities.

IAF management indicated that the COOP Plan was not updated since April 2015 due to a change in contractors. IAF awarded a contract to a new vendor to host the COOP function. The hardware was in the process of being moved to the new location and IAF planned to perform a contingency test after the move.

Without an up-to-date contingency plan, IAF is at risk of not being able to adequately return to business operations after an emergency or natural disaster. Additionally, lack of contingency plan testing increases the likelihood that the contingency plans in place will not function appropriately. As a result, we recommend the following:

***Recommendation 8:*** *We recommend that the Inter-American Foundation's Chief Information Officer document an updated continuity of operations plan to include a business impact analysis.*

***Recommendation 9:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a validation process to ensure annual testing of the continuity of operations plan is performed.*

## 8. IAF Needs to Strengthen the Plans of Action and Milestones Process

NIST Special Publication 800-53, Revision 4, security control CA-5, states the following regarding the plans of action and milestones:

> The organization:
> * * *
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Plans of Action and Milestones (POA&Ms) had not been updated to reflect their current status and not all findings had been incorporated into POA&Ms. Specifically, there were four POA&M items from Fiscal Year 2014 that had been completed, but the items were still noted as open. In addition, findings that were identified in the security assessment report dated April 2015, were not included in the POA&M report for tracking of milestones and corrective actions.

IAF was trying to use different formats to track POA&M items; however, the new format did not incorporate the status of prior year findings and findings from the security assessment.

Without documenting and tracking all known system security control weaknesses and their associated corrective actions in the POA&Ms, IAF cannot effectively manage system security risks associated with their systems. As a result, we recommend the following:

> ***Recommendation 10:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement a written process to validate whether the plans of action and milestones is completed and updated timely and includes all applicable control weaknesses.*

## 9. IAF Needs to Update the Standard Operating Procedures to Include Privacy Controls

NIST Special Publication 800-53, Revision 4, security control PL-1, states the following regarding planning:

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

The *Information System Security Program Standard Operating Procedures (SOP)* did not reflect NIST Special Publication 800-53, Revision 4, controls related to the Privacy Controls Family. IAF management updated the SOP to reflect to NIST SP 800-53, Revision 4; however, the privacy controls were not included in the updated SOP. Management indicated that since IAF did not maintain Personally Identifiable Information (PII) on the Enterprise Network, policies and procedures covering privacy would not be necessary.

Without documenting privacy control implementation, IAF maybe not be providing all the necessary safeguards to protect PII.

> ***Recommendation 11:*** *We recommend that the Inter-American Foundation's Chief Information Officer update and implement the* Information System Security Program Standard Operating Procedures *to include the privacy controls identified in NIST Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations*.*

## 10. IAF Needs to Update the Enterprise Network System Security Plan

NIST Special Publication 800-53, Revision 4, security control PL-2, states the following regarding planning:

> The organization:
>
> a. Develops a security plan for the information system that:
>
> * * *
>
> 5. Describes the operational environment for the information system and relationships with or connections to other information systems.

The *IAF Enterprise Network and Software Applications System Security Plan* did not accurately reflect or did not have adequate information to reflect the current operating environment. Examples include, but not limited to:

- The privacy and program management controls had not been documented.
- CP-2, Alternate Processing Site control did not indicate the correct location of the alternate site location.
- Section 1.10 details the information system component inventory; however, it did not reflect the current inventory.
- CA-7, Continuous Monitoring control indicates that IAF continuously monitors its system to ensure on-going security; however, we noted that IAF is still in process of obtaining a license for their continuous monitoring solution.

IAF management indicated while performing annual updates some areas may have been overlooked or missed.

Without a complete and current system security plan, security responsibilities and controls are not appropriately documented, disseminated, implemented, or monitored; therefore, IAF systems may be more susceptible to improper access, use, or loss of sensitive information. Therefore, we recommend the following:

> ***Recommendation 12:*** *We recommend that the Inter-American Foundation's Chief Information Officer update the* IAF Enterprise Network and Software Applications System Security Plan *to reflect the current operating environment.*

## 11. External Information System Agreements Need to be Current

NIST Special Publication 800-53, Revision 4, security control CA-3, states the following regarding interconnection security agreements:

> The organization:
>
> * * *
>
> b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated;

c. Reviews and updates the Interconnection Security Agreements [Assignment: organization-defined frequency].

The Interconnection Security Agreement (ISA) between IAF and the Department of Interior (DOI)/Interior Business Center (IBC) expired on January 17, 2016. This agreement addresses the interconnection between the two party's networks for the purposes of providing IAF's users with access to the Federal Personnel and Payroll System and the connections within IAF's network. IAF submitted the ISA to DOI on April 15, 2016; however, DOI had not provided IAF with a current signed agreement.

Without an agreement, security controls to protect the confidentiality, integrity, and availability of the DOI/IBC and IAF systems and the data transferred between them are not documented, increasing the risk that adequate security over IAF data will not be implemented. In addition, when system interfaces are not accurately understood and documented there is an increased risk that data may be added, lost, or altered during processing. As a result, we recommend the following:

***Recommendation 13:*** *We recommend that the Inter-American Foundation Chief Information Officer obtain a written, fully executed Interconnection Security Agreement with the Department of Interior's Interior Business Center.*

## 12. Information System Inventory Needed to be Documented

NIST Special Publication 800-53, Revision 4, security control PM-5, states the following regarding information system inventory:

> The organization develops and maintains an inventory of its information systems.

Additionally, the Federal Information Security Management Act of 2002 states the following regarding information system inventory:

> c) Inventory of Major Information Systems.—
> (1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.
> (2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.
> (3) Such inventory shall be—
> (A) updated at least annually

IAF did not maintain an inventory of information systems to include internal and contractor systems and applications. Management was not aware of the FISMA requirement that a complete information system inventory needed to be maintained.

Without an inventory of information systems, there is an increased risk that security controls will not be appropriately implemented and monitored for all systems. Upon notification of the issue, IAF took action to correct this weakness. Therefore, we are not making a recommendation at this time.

## 13. Account Management Controls need to be Strengthened

NIST Special Publication 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization develops:
>
> * * *
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*].

IAF did not disable GEMS user accounts after 90 days of inactivity. Specifically, one user account from a population of 21 user accounts remained active after 90 days of inactivity. IAF management indicated the script used to identify inactive accounts only identifies accounts with last logon dates greater than 90 days but does not disable the accounts. The IAF Chief Information Officer indicated the Office Directors require access to the application for reviewing inactive user reports; however, the access was used infrequently.

Without disabling inactive user accounts there is an increased risk of unauthorized access. Upon notification of the issue, IAF management took action to correct this weakness and documented an exemption for specific user accounts to not be disabled. Therefore, we are not making a recommendation at this time.

# EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Inter-American Foundation (IAF) outlined its plans to address all 13 recommendations and described planned actions to address the recommendations. IAF's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on all 13 recommendations, though we disagree that final action has been taken on recommendation 6. Further, we acknowledge final action has been taken on recommendation 13.

In response to recommendation 6, IAF noted they have implemented log monitoring software on and a security information and event management tool. In addition, IAF indicated that procedures had been established for the periodic review of auditable events. We acknowledge IAF's management decision on recommendation 6. However, because the log monitoring and analysis was not fully implemented and configured at the time of our testing, and to ensure the control is in place and operating effectively, an independent verification of the tool and processes has to be done. Therefore, final action has not yet been completed on recommendation 6.

In response to recommendation 13, IAF obtained an extension of the current Interconnection Security Agreement with the Department of Interior's Interior Business Center. Therefore, we acknowledge final action has been taken on recommendation 13.

# SCOPE AND METHODOLOGY

## Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe 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 the Inter-American Foundation implement selected security for selected information systems[4] in support of the Federal Information Security Modernization Act of 2014.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 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:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Physical and Environmental
- Planning
- Personnel Security
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communication Protection
- System and Services Acquisition
- Transparency

For this audit we reviewed two IAF-managed information systems, the Enterprise Network and the Grants Evaluation and Management System, and one contractor system, Google Mail. See Appendix III for a listing of selected controls for each system. The audit also included a vulnerability assessment of IAF's general support system and an evaluation of IAF's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit

[4] See Appendix III for a list of controls and systems selected.

recommendations[5] to determine if IAF made progress in implementing the recommended improvements concerning its information security program.

The audit was conducted at IAF's headquarters in Washington, D.C., from April 6, 2016 through August 5, 2016.

## Methodology

Following the framework for minimum security controls in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, certain controls (listed in Appendix III) were selected from NIST security control families.[6] We reviewed the selected controls[7] over IAF's Enterprise Network, the Grants Evaluation and Management System, and IAF's contractor system, Google Mail.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.

- Reviewed documentation related to IAF's information security program, such as security policies and procedures, system security plans, and risk assessments.

- Tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix III).

- Reviewed the status of recommendations in the fiscal year 2015 FISMA audit report.[8]

- Completed a network vulnerability assessment of IAF's general support system.

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality 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 percentage of deficient items found compared to the total population available for review.

In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected, and if projected, may be misleading.

[5] *Audit of the Inter-American Foundation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-IAF-15-008-P, September 11, 2015).
[6] Security controls are organized into families according to their security function—for example, access controls.
[7] See Appendix III for a list of controls and systems selected.
[8] ibid. footnote 5.

# MANAGEMENT COMMENTS

Inter-American Foundation
An Independent Agency of the U.S. Government

October 21, 2016

**MEMORANDUM**

**TO:** IG/A/ITA, Mark Norman, Director

**FROM:** IAF, Rajiv Jain, Chief Information Officer

**SUBJECT:** Follow-Up Action on Recommendations from USAID OIG Audit Report No. - A-IAF-16-001-P dated September 14, 2016

This memorandum provides a status update on actions taken to address the recommendations contained in the Audit of the Inter-American Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2016, Audit Report No. A-IAF-16-001-P.

***Recommendation 1:*** *We recommend that the Inter-American Foundation's Chief Information Officer either (1) remediate vulnerabilities in the network identified by the Office of Inspector General's contractor, as appropriate, and document the results or (2) document acceptance of the risks of those vulnerabilities.*

Completed:

1. IAF is aggressively patching computers and laptops with updates and patches; 9/1/2016

In response to Recommendation 1, IAF has proposed the following actions and a target date to mitigate findings on the recommendation

1. IAF will procure and refresh new servers that will replace the current database server and oracle application server that is running Windows 2003. The new servers will run Windows 2008 and will be Microsoft supported and under compliance – 3/31/2017
2. IAF will review the SMB shares and adjust the access privileges as required – 11/15/2016

Target date for completion: 3/31/2017

***Recommendation 2:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement a continuous monitoring plan and program.*

Completed:
IAF has implemented Logic Monitor (pre-built mechanism to automate monitoring and alerting on infrastructure and applications) on June 6th, 2016 and Alien Vault (Security information and event management tool SIEM) on September 26, 2016. IAF collects reports on a weekly basis and monitors events in real time and an email ticket is created in IAF Helpdesk system. IAF also performs regular vulnerability scanning for all the devices on the network.

In response to Recommendation 2, IAF proposes the following action items to mitigate findings:

1. IAF will develop and document a formal continuous monitoring plan consistent with FISMA requirements. The plan will identify key tools and events and define a process for monitoring, taking action and reporting on events of interest.
2. IAF has procured change control management tool/application and is in the implementation process.

Target completion date: 12/30/2016

***Recommendation 3:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement monitoring controls of baseline configurations for the Enterprise Network and document the results.*

Completed:
1. IAF performed baseline scan for Windows 2007 using USGCB standards; 9/30/2016
2. IAF performed baseline scan for Windows Server 2008 using CIS benchmark; 9/30/2016
3. IAF procured change management tool/application "Net results tracker" for change management process; 9/30/2016

In response to Recommendation 3, IAF proposes the following actions and a target date to mitigate findings:

1. IAF will establish a formal baseline for enterprise network technologies.
2. IAF will document a formal change control process to approve changes to established baselines.
3. IAF will perform a periodic check against approved configuration baselines to identify unauthorized changes and take remediation steps as appropriate.

Target completion date: 12/30/2016

***Recommendation 4:*** *We recommend that the Inter-American Foundation's Chief Information Officer complete a system risk assessment for the Enterprise Network that takes into account all known vulnerabilities, threat sources, and security controls planned or in place, and determine the resulting level of residual risk to ensure the authorizing official has appropriate knowledge of the security state of the information system.*

In response to Recommendation 4, IAF proposes the following actions and a target date to mitigate findings:

1. IAF to perform risk assessment (RA) of its information systems and technology including systems test and evaluation for the authorizing official. The report will provide the security state of IAF systems.

Target completion date: 3/30/2017

***Recommendation 5:*** *We recommend that the Inter-American Foundation's Chief Information Officer obtain a current authorization to operate for the Enterprise Network that is based on a completed security controls assessment and updated system security plan, risk assessment and plan of action and milestones.*

In response to Recommendation 5, IAF proposes the following actions to address the finding:

1. Update system security plan
2. Update risk assessment
3. Update plan of action and milestones (POAM)

Target completion date: 3/30/2017

***Recommendation 6:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to review and analyze auditable events.*

In response to Recommendation 6, IAF management has taken following actions and consequently final action has been taken on the recommendation:

1. IAF established procedures for the periodic review of auditable events.
2. IAF implemented Logic Monitor (pre-built mechanism to automate monitoring and alerting on infrastructure and applications) on June 6th, 2016 and Alien Vault (Security information and event management tool SIEM) on September 26, 2016.
3. As of Aug 8, 2016 IAF collects reports on a weekly basis and monitors events in real time and an email ticket is created in IAF Helpdesk system. IAF will periodically fine tune auditable events to focus attention on the greatest risk areas.

Date implemented: 9/30/2016

***Recommendation 7:*** *We recommend that the Inter-American Foundation's Chief Information Officer implement multifactor authentication for all network accounts and document the results.*

In response to Recommendation 7, IAF proposes the following actions to address the finding.

1. Research multi factor authentication solutions available and suitable for IAF including PIV.
2. Implement solution

Target completion date: 6/30/2018

***Recommendation 8:*** *We recommend that the Inter-American Foundation's Chief Information Officer document an updated continuity of operations plan to include a business impact analysis.*

In response to Recommendation 8, IAF proposes the following actions to address the finding:

1. Update continuity of operations plan
2. Document business impact analysis

Target completion date: 12/30/2016

***Recommendation 9:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a validation process to ensure annual testing of the continuity of operations plan is performed.*

Completed:

1. In June 2016 IAF management procured / leased a COOP site under the agency name so that the COOP site does not keep changing when the contractors change hands.

2. IAF IT staff along with the contractors have completed a table-top exercise with the disaster scenario in mind. (The exercise is based on National Institute of Standards and Technology (NIST) Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems, Rev. 1. NIST SP 800-34 Rev. 1 provides instructions, recommendations and considerations for government IT contingency planning. The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at [IAF – EN and GEMS] following an event causing the outage of mission critical systems that are housed in the [1331 Pennsylvania AVE, Washington DC]. This exercise is designed to improve the readiness of the [IAF – EN and GEMS] and help validate existing ISCP procedures.); 5/6/2016

3. IAF has completed the setup of hardware at the new COOP site; 9/16/2016

In response to Recommendation 9, IAF proposes the following actions to address the finding:

1. Conduct annual testing and document results for IAF's continuity of operations.

Target completion date: 12/30/2016

***Recommendation 10:*** *We recommend that the Inter-American Foundation's Chief Information Officer develop and implement a written process to validate whether the plans of action and milestones is completed and updated timely and includes all applicable control weaknesses.*

In response to Recommendation 10, IAF proposes the following action to address the finding:

1. IAF will review the POAM document after each scan to update and close the vulnerabilities.
2. IAF will review the POAM document after assessments, System tests, and audits and update the POAM accordingly.

Target date of completion: 12/30/2016

***Recommendation 11:*** *We recommend that the Inter-American Foundation's Chief Information Officer update and implement the* Information System Security Program Standard Operating Procedures *to include the privacy controls identified in NIST Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations*.*

In response to Recommendation 9, IAF proposes the following actions to address the finding:

1. Update system security plan
2. Update the IAF's standard operating procedures manual to include the privacy controls identified in NIST 800-53, rev 4.

Target completion date: 3/30/2017

***Recommendation 12:*** *We recommend that the Inter-American Foundation's Chief Information Officer update the* IAF Enterprise Network and Software Applications System Security Plan *to reflect the current operating environment.*

In response to Recommendation 12, IAF proposes the following actions to address the finding:

1. Update IAF Enterprise Network and Software Applications System Security Plan to reflect the current operating environment
2. Review the document

Target completion date: 3/30/2017

***Recommendation 13:*** *We recommend that the Inter-American Foundation Chief Information Officer obtain a written, fully executed Interconnection Security Agreement with the Department of Interior's Interior Business Center.*

In response to Recommendation 13, IAF management has taken following actions and consequently final action has been taken on the recommendation:

1. IAF received an extension memo for the existing ISA from Department of Interior in lieu of a new Interconnection Security Agreement (ISA).

Completion date: 8/15/2016

We are continually seeking ways in which to further strengthen the Inter-American Foundation's IT security infrastructure and posture, and we value the advice and support provided by the Office of the Inspector General in assisting us in that goal.

Sincerely,

/s/

Rajiv Jain
CIO, Inter-American Foundation.
202-803-6107

# Summary of Results for Each Control Reviewed

| Control | Control Name | Is Control Effective |
|---|---|---|
| **Enterprise Network** | | |
| AC-1 | Access Control Policy & Procedures | Yes |
| AC-2 | Account Management | Yes |
| AC-3 | Access Enforcement | Yes |
| AC-4 | Information Flow Enforcement | Yes |
| AC-5 | Separation of Duties | Yes |
| AC-6 | Least Privilege | Yes |
| AC-7 | Unsuccessful Login Attempts | Yes |
| AC-8 | Systems Use Notification | Yes |
| AC-11 | Session Lock | Yes |
| AC-17 | Remote Access | Yes |
| AC-19 | Access Control for Mobile Devices | Yes |
| AC-20 | Use of External Information Systems | Yes |
| AT-1 | Security Awareness & Training Policy and Procedures | Yes |
| AT-2 | Security Awareness | Yes |
| AT-3 | Security Training | Yes |
| AT-4 | Security Training Records | Yes |
| AU-6 | Audit, Review, Analysis and Reporting | No, See finding 5 |
| CA-1 | Security Assessment and Authorization Policies and Procedures | Yes |
| CA-2 | Security Assessments | Yes |
| CA-3 | System Interconnections | No, See finding 11 |
| CA-5 | Plan of Action and Milestones | No, See finding 8 |
| CA-6 | Security Accreditation | No, See finding 4 |
| CA-7 | Continuous Monitoring | No, See finding 2 |
| CA-9 | Internal System Connections | Yes |
| CM-1 | Configuration Management Policy & Procedures | Yes |
| CM-2 | Baseline Configuration | No, See finding 3 |
| CM-3 | Configuration Change Control | Yes |
| CM-4 | Security Impact Analysis | Yes |
| CM-6 | Configuration Settings | Yes |
| CM-7 | Least Functionality | Yes |
| CM-8 | Information System Component Inventory | Yes |
| CP-1 | Contingency Planning Policy & Procedures | Yes |
| CP-2 | Contingency Plan | No, See finding 7 |
| CP-4 | Contingency Plan Testing and Exercises | No, See finding 7 |
| CP-6 | Alternate Storage Sites | Yes |
| CP-7 | Alternate Processing Sites | Yes |
| CP-8 | Telecommunication Services | Yes |

| Control | Control Name | Is Control Effective |
|---|---|---|
| CP-9 | Information System Backup | Yes |
| CP-10 | Information System Recovery & Reconstitution | Yes |
| IA-1 | Identification & Authentication Policy and Procedures | Yes |
| IA-2 | User Identification & Authentication (Organizational Users) | No, See finding 6 |
| IA-3 | Device Identification & Authentication | Yes |
| IA-4 | Identifier Management | Yes |
| IA-5 | Authentication Management | Yes |
| IR-1 | Incident Response Policy & Procedures | Yes |
| IR-4 | Incident Handling | Yes |
| IR-5 | Incident Monitoring | Yes |
| IR-6 | Incident Reporting | Yes |
| IR-8 | Incident Response Plan | Yes |
| PE-14 | Temperature and Humidity Controls | Yes |
| PL-1 | Security Planning Policy & Procedures | No, See finding 9 |
| PL-2 | System Security Plan | No, See finding 10 |
| PS-4 | Personnel Termination | Yes |
| PS-6 | Access Agreements | Yes |
| RA-1 | Risk Assessment Policy and Procedures | Yes |
| RA-2 | Security Categorization | Yes |
| RA-3 | Risk Assessment | Yes |
| RA-5 | Vulnerability Scanning | No, See finding 1 |
| SA-1 | System & Services Acquisition Policy and Procedures | Yes |
| SA-4 | Acquisitions Process | Yes |
| SA-5 | Information System Documentation | Yes |
| SA-9 | External Information System Services | Yes |
| SA-10 | Developer Configuration Management | Yes |
| SA-11 | Developer Security Testing and Evaluation | Yes |
| SC-7 | Boundary Protection | Yes |
| SC-8 | Transmission Confidentiality and Integrity | Yes |
| SI-2 | Flaw remediation | Yes |
| PM-1 | Information Security Program Plan | Yes |
| PM-3 | Information Security Resources | Yes |
| PM-4 | Plan Of Action And Milestones Process | Yes |
| PM-5 | Information System Inventory | No, See finding 12 |
| PM-6 | Information Security Measures Of Performance | Yes |
| PM-7 | Enterprise Architecture | Yes |
| PM-8 | Critical Infrastructure Plan | Yes |
| PM-9 | Risk Management Strategy | Yes |
| PM-10 | Security Authorization Process | Yes |
| AR-1 | Governance and Privacy Program | Yes |
| AR-2 | Privacy Impact and Risk Assessment | Yes |
| TR-1 | Privacy Notice | Yes |
| TR-3 | Dissemination of Privacy Program Information | Yes |
| **Grants Evaluation and Management System** | | |
| AC-1 | Access Control Policy & Procedures | Yes |
| AC-2 | Account Management | No, See finding 13 |
| AC-5 | Separation of Duties | Yes |

| Control | Control Name | Is Control Effective |
|---|---|---|
| AC-7 | Unsuccessful Login Attempts | Yes |
| AU-6 | Audit, Review, Analysis and Reporting | Yes |
| CM-2 | Baseline Configuration | Yes |
| CP-2 | Contingency Plan | Yes |
| CP-4 | Contingency Plan Testing and Exercises | Yes |
| CP-7 | Alternate Processing Sites | Yes |
| CP-9 | Information System Backup | Yes |
| RA-5 | Vulnerability Scanning | Yes |
| **Google Mail** | | |
| CM-2 | Baseline Configuration | Yes |
| CP-2 | Contingency Plan | Yes |
| CP-4 | Contingency Plan Testing and Exercises | Yes |
| CP-9 | Information System Backup | Yes |
| RA-2 | Security Categorization | Yes |
| RA-3 | Risk Assessment | Yes |
| SA-4 | Acquisitions Process | Yes |

# Status of Prior Year Findings

The following table provides the status of the FY 2015 FISMA Audit Recommendations.[9]

| No. | FY 2015 Audit Recommendation | IAF Status | Auditor's Position on Status |
|---|---|---|---|
| 1 | We recommend that the Inter-American Foundation Chief Information Officer either (1) remediate vulnerabilities in the network identified by the Office of Inspector General's contractor, as appropriate, and document the results or (2) document acceptance of the risks of those vulnerabilities. | Closed | Agree. Although this audit noted weaknesses (Finding #1), IAF corrected the weaknesses identified in the FY 2015 FISMA Audit. |
| 2 | We recommend that the Inter-American Foundation Chief Information Officer develop and implement a documented process to validate the completeness of the vulnerability scans to determine whether all applicable vulnerabilities are identified and either remediated or accepted in a timely manner. | Closed | Agree |
| 3 | We recommend that the Inter-American Foundation Chief Information Officer document and implement procedures to review active network accounts that have not logged in over a specified period of time, as defined by the Foundation, to determine whether accounts are necessary. | Closed | Agree |
| 4 | We recommend that the Inter-American Foundation Chief Information Officer document and implement a process to review service and administrator accounts to determine whether passwords are changed within Foundation defined periods. | Closed | Agree |
| 5 | We recommend that the Inter-American Foundation's Chief Information Officer update and implement the Information System Security Program Standard Operating Procedures to reflect NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. | Closed | Agree. Although this audit noted weaknesses (Finding #9), IAF corrected most weaknesses identified in the FY 2015 FISMA Audit. |
| 6 | We recommend that the Inter-American Foundation's Chief Information Officer develop and implement a documented process to review and update the IAF Enterprise Network and Software Applications System Security Plan on an annual basis. At a minimum, this should include a determination whether the security requirements and controls for the system are adequately documented and reflect the current information system environment. | Closed | Agree. Although this audit noted weaknesses (Finding #10), IAF corrected most weaknesses identified in the FY 2015 FISMA Audit. |

[9] ibid. footnote 5.

| No. | FY 2015 Audit Recommendation | IAF Status | Auditor's Position on Status |
|---|---|---|---|
| 7 | We recommend that the Inter-American Foundation's Chief Information Officer implement multi-factor authentication with one factor separate from the system gaining access for the Foundation's use of Google Mail. | Closed | Agree |
| 8 | We recommend that the Inter-American Foundation's Chief Information Officer implement monitoring controls of humidity levels in the computer room and document the results. | Closed | Agree |
| 9 | We recommend that the Inter-American Foundation's Chief Information Officer update the privacy notice on the Foundation's public website to include:<br><br>• The choices, if any, individuals may have regarding how the organization uses personally identifiable information (PII) and the consequences of exercising or not exercising those choices;<br>• The ability to access and have PII amended or corrected if necessary;<br>• PII the organization collects and the purpose(s) for which it collects that information;<br>• How the organization uses PII internally;<br>• Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;<br>• Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; and<br>• How individuals may obtain access to PII and how the PII will be protected. | Closed | Agree |

**U.S. Agency for International Development**
**Office of Inspector General**
1300 Pennsylvania Avenue NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
oig.usaid.gov
Audit Task No. AA100916