OFFICE OF INSPECTOR GENERAL
Inter-American Foundation

# IAF Has Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed

**AUDIT REPORT A-IAF-18-002-C**
**OCTOBER 02, 2017**

1300 Pennsylvania Avenue NW • Washington, DC 20523
oig.usaid.gov • 202-712-1150

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

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

## Report waste, fraud, and abuse

**Inter-American Foundation Hotline**
Email: iafhotline@usaid.gov
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, Attn: IAF Hotline, P.O. Box 657, Washington, DC 20044-0657

# MEMORANDUM

**DATE:** October 02, 2017

**TO:** President and CEO, IAF, Paloma Adams-Allen

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

**SUBJECT:** IAF Has Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed (A-IAF-18-002-C)

Enclosed is the final audit report on the Inter-American Foundation's (IAF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2017. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. The contract required Clifton to perform the audit in accordance with generally accepted government auditing standards.

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

The audit objective was to determine whether IAF implemented certain security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested IAF's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Clifton reviewed selected controls from IAF's two internal information systems and one of five external systems. The firm also performed a vulnerability assessment of IAF's general support system and an evaluation of IAF's process for identifying, correcting, and mitigating technical vulnerabilities. Fieldwork was performed at IAF's headquarters in Washington, DC, from March 29 through August 1, 2017.

Clifton concluded that IAF implemented 86 of 94 selected security controls that were designed to preserve the confidentiality, integrity, and availability of its information and information systems. For example, IAF did the following:

- Implemented an effective process to monitor, review, and analyze audit logs.
- Maintained effective change management policies and procedures.
- Implemented effective security awareness and training procedures.
- Maintained adequate audit log monitoring.
- Maintained adequate processing procedures for bringing on new employees and timely removal of access for terminated employees.

However, IAF did not implement eight controls. To address the weaknesses identified in the report, Clifton made and OIG agrees with the following recommendations to IAF's management. We will track them until fully implemented. We recommend IAF's chief information officer:

**Recommendation 1.** Remediate unsupported software and configuration-related vulnerabilities in the network identified by the Office of Inspector General, as appropriate, and document the results, or document acceptance of the risks of those vulnerabilities.

**Recommendation 2.** Document and implement a process to test system changes and document the results of testing.

**Recommendation 3.** Document and implement a process to test the Foundation's incident response capabilities.

In finalizing the report, Clifton evaluated IAF's responses to the recommendations. Both Clifton and OIG acknowledge IAF's management decisions on recommendations 1 through 3.

We appreciate the assistance extended to our staff and Clifton employees during the engagement.

# The Inter-American Foundation Has Implemented Many Controls in Support of the Federal Information Security Modernization Act of 2014, But Improvements Are Needed

## Fiscal Year 2017

## Final Report

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203

571-227-9500 | fax 571-227-9552

CLAconnect.com

CliftonLarsonAllen

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

September 25, 2017

Mr. Mark S. 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 (IAF) 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 certain 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 selected controls from IAF's 2 internal information systems and from 1 of 5 external systems. 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. Audit fieldwork was performed at the Inter-American Foundation's headquarters in Washington, D.C., from March 29, 2017 through August 1, 2017.

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 many selected security controls for selected information systems. Although IAF generally had policies for its information security program, its implementation of those policies for a subset of 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 three recommendations to assist IAF in strengthening its information security program. In addition, findings related to four recommendations from prior years were not yet fully implemented and therefore new recommendations were not made.

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 the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

# TABLE OF CONTENTS

# SUMMARY OF RESULTS

The Federal Information Security Modernization Act of 2014[1] (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 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) a 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 to 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 certain 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 selected controls from IAF's two internal information systems and from one of five external systems. The systems included general support systems and major applications.

### Results

The audit concluded that IAF generally complied with FISMA requirements by implementing 86 of 94 selected security controls for selected information systems. For example, IAF:

- Maintained effective change management policy and procedures.
- Implemented effective security awareness and training procedures.

[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 II for a list of controls.

- Maintained adequate audit log monitoring.

- 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 8 of the 94 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 system vulnerabilities.

- Document testing of information system changes.

- Test incident response plans.

- Strengthen the security assessment and authorization process and assess system risks.

- Implement multi-factor authentication.

- Update the continuity of operation plan.

As a result, IAF's operations and assets may be at risk of unauthorized access, misuse and disruption. This report makes three recommendations to assist IAF in strengthening its information security program. In addition, findings related to four recommendations from prior years were not yet fully implemented and therefore new recommendations were not made. Based on our evaluation of management comments, we acknowledge management decisions on all recommendations. IAF's comments are included in their entirety in Appendix II.

Detailed findings appear in the following section.

# 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 SI-2, states the following regarding flaw remediation:

> The organization:
>
> a. Identifies, reports, and corrects information system flaws.
>
> * * *
>
> c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

IAF had a process in place to remediate vulnerabilities within patch cycles. However, independent scans performed using the software tool Nessus noted critical and high risk vulnerabilities related to patch management, configuration management and unsupported software. Many of the patch management vulnerabilities were publicly known before 2016.

IAF has taken a more targeted approach at vulnerability remediation and is targeting individual computers to patch; however, vulnerabilities continue to exist due to the nature of IAF's business. Specifically, some users were traveling abroad and their computers were not receiving the security updates.

In addition, IAF was continuing to use unsupported software and configuration weaknesses that were not addressed by patching which accounted for the majority of older vulnerabilities.

Unmitigated vulnerabilities on IAF's network can compromise the confidentiality, integrity, and availability of IAF data. 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 remediate unsupported software and configuration related vulnerabilities in the network identified by the Office of Inspector General, as appropriate, and document the results or document acceptance of the risks of those vulnerabilities.*

## 2. IAF Needs to Document Testing of System Changes

NIST Special Publication 800-53, Revision 4, security control CM-3, control enhancement 2, states that the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Of the 17 closed system changes, two of three sampled changes did not have documented test results. IAF indicated that the changes were tested and the results were reviewed because the changes had been approved for release to production, but that the process had not been documented. IAF management indicated that they will now modify change tickets to begin documenting the testing of changes and associated test results.

By not adequately testing the changes to the information systems, IAF increases the risk that insecure or deficient changes may be implemented and may adversely impact the production environment. As a result, we recommend the following:

> ***Recommendation 2:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test system changes and document the results of testing.*

## 3. IAF Needs to Test Incident Response Plans

NIST Special Publication 800-53, Revision 4, security control IR-3, states the organization tests the incident response capability for the information system *[Assignment: organization-defined frequency]* using *[Assignment: organization-defined tests]* to determine the incident response effectiveness and documents the results.

IAF indicated that they performed an incident response table top test in December 2016. The test was coordinated with personnel responsible for the system's incident response and related plans. However, IAF did not document incident response testing plans or the testing results. Therefore, the testing of the incident response capabilities could not be evaluated during the audit period.

By not testing the incident response plans and procedure, IAF increases the risk that they may not have an adequate response should an incident occur. As a result, we recommend the following:

> ***Recommendation 3:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test the Foundation's incident response capabilities.*

## 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, security control RA-3, states the following regarding risk assessments:

> The organization:
>
> * * *
>
> d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Further, security control CA-2, states the following regarding security assessments:

> The organization:
>
> * * *
>
> b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 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."

One system 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 delays in identifying and assigning an authorizing official. IAF management indicated they expect the security assessment and updated risk assessment to be completed by September 30, 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.

Recommendations addressing this finding were issued in the fiscal year 2016 FISMA audit.[3] Specifically, the Authorization to Operate was invalid, the Security Assessment and Risk Assessment were outdated, and the recommendations from fiscal year 2016 remain open. Therefore, we are not making an additional recommendation at this time.

## 5. IAF Needs to Implement Multi-factor Authentication

NIST Special Publication 800-53, Revision 4, security control IA-2, states the organization should implement multifactor authentication 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) requires the use of Personal Identification Verification for gaining logical access to federally controlled information systems.

IAF did not implement multifactor authentication for its privileged and non-privileged users. Multifactor authentication was only implemented for remote access. IAF had purchased equipment capable of accepting Personal Identify Verification (PIV) cards; however, management indicated they have experienced technical difficulties during implementation. IAF has targeted to have PIV enabled authentication by June 2018.

By not fully implementing multifactor authentication, IAF increases the risk that unauthorized individuals could gain access to its information system and data.

A recommendation addressing this finding was issued in the fiscal year 2016 FISMA audit.[4] IAF plans to take final corrective action by June 2018. Therefore, we are not making an additional recommendation at this time.

## 6. Continuity of Operations Plan Needs to be Updated

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

> The organization:
>
> a. Develops a contingency plan for the information system that:
>
> * * *
>
> 2. Provides recovery objectives, restoration priorities, and metrics;
>
> * * *
>
> 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

[3] Recommendations 4 and 5, *The Inter-American Foundation has Implemented Many Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-IAF-17-004-C, November 7, 2016).

[4] Recommendation 7, *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).

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

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.

IAF management indicated they were in the process of awarding a contract for hosting the backup infrastructure in Microsoft's Azure cloud environment. The cloud environment would replace IAF's current backup infrastructure site located in Ashburn, Virginia which has not been fully tested for infrastructure recovery. IAF indicated that the business impact analysis is expected to be completed by September 30, 2017.

Without a complete 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 a complete and accurate contingency plan increases the likelihood that the contingency plans in place will not function appropriately.

A recommendation addressing this finding was issued in the fiscal year 2016 FISMA audit.[5] However, the Continuity of Operations Plan had not been fully updated and the recommendation from the prior year remains open. Therefore, we are not making an additional recommendation at this time.

[5] Recommendation 8, *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).

# EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Inter-American Foundation (IAF) described planned actions to address all three 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 three recommendations.

# 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 IAF implemented selected security for certain information systems[6] 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 (NIST) 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
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Planning
- Personnel Security
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communication Protection
- System and Services Acquisition
- System and Information Integrity
- Accountability, Audit and Risk Management

For this audit we reviewed selected controls from IAF's 2 internal information systems and from 1 of 5 external systems. The systems included general support systems and major applications. See Appendix II for a listing of selected controls. 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 recommendations[7] to determine if IAF made progress in implementing the recommended improvements concerning its information security program.

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

[7] *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).

The audit was conducted at IAF's headquarters in Washington, D.C., from March 29, 2017 through August 1, 2017.

## Methodology

Following the framework for minimum security controls in NIST Special Publication 800-53, Revision 4, certain controls (listed in Appendix II) were selected from NIST security control families.[8] We reviewed the selected controls[9] over 2 of IAF's internal information systems and from 1 of 5 external systems.

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.

- Reviewed the status of recommendations in the fiscal year 2016 FISMA audit report.[10]

- Completed a network vulnerability assessment.

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.

[8] Security controls are organized into families according to their security function—for example, access controls.

[9] See Appendix II for a list of controls.

[10] ibid. footnote 8.

# Management Comments

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

September 18, 2017

**MEMORANDUM**

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

**CC:** Lesley Duncan, COO, Inter-American Foundation

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

**SUBJECT:** Follow-Up Action on Recommendations from USAID OIG Audit Report No. A-IAF-17-00X-C dated September 11, 2017

This memorandum provides a status update on actions planned and taken to address the recommendation contained in the Audit of the Inter-American Foundation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2017, Audit Report A-IAF- 17-00X-C dated September 11, 2017.

***Recommendation 1:*** *We recommend that the Inter-American Foundation's chief information officer remediate unsupported software and configuration related vulnerabilities in the network identified by the Office of Inspector General, as appropriate, and document the results or document acceptance of the risks of those vulnerabilities.*

In response to Recommendation 1, IAF proposes the following action items and a target date to mitigate the finding.

1. IAF has updated unsupported software such as Cisco VPN client and Adobe, completed August 2017. IAF will remove un-supported software and files from user workstations that appear on the scan results; October 2017.
2. 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, November 2017
3. IAF identifies staff who have missed the patch cycle and follows up with the individual to receive the latest patches.

Target date: 12/30/2017

***Recommendation 2:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test system changes and document the results of testing.*

In response to Recommendation 2, IAF management proposes a target date and the following action items to mitigate the finding:

1. IAF will review existing process and update procedures requiring maintenance of test artifacts.
2. IAF will document the test cases and changes in the change control application for approval and documentation.

Target date: 10/30/2017

***Recommendation 3:*** *We recommend that the Inter-American Foundation's Chief Information Officer document and implement a process to test the Foundation's incident response capabilities.*

In response to Recommendation 3, IAF has performed the following action item and consequently final action has been taken on the recommendation:

1. IAF completed table top exercise that simulated a cyber security incident.
2. IAF followed the procedures from the Incident response plan document.
3. An after action report was created.

Completed date: 9/5/2017

(The supplementary documents will be uploaded via the SFTP site)

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.

# Number of Controls Reviewed for Each System

| Control | Control Name | Number of Systems Tested |
|---|---|---|
| AC-1 | Access Control Policy & Procedures | 1 |
| AC-2 | Account Management | 2 |
| AC-3 | Access Enforcement | 1 |
| AC-4 | Information Flow Enforcement | 1 |
| AC-5 | Separation of Duties | 1 |
| AC-6 | Least Privilege | 1 |
| AC-11 | Session Lock | 1 |
| AC-12 | Session Termination | 1 |
| AC-17 | Remote Access | 1 |
| AC-19 | Access Control for Mobile Devices | 1 |
| AC-20 | Use of External Information Systems | 3 |
| AT-1 | Security Awareness & Training Policy and Procedures | 1 |
| AT-2 | Security Awareness | 1 |
| AT-3 | Security Training | 1 |
| AT-4 | Security Training Records | 1 |
| CA-1 | Security Assessment and Authorization Policies and Procedures | 1 |
| CA-2 | Security Assessments | 1 |
| CA-3 | System Interconnections | 3 |
| CA-5 | Plan of Action and Milestones | 1 |
| CA-6 | Security Accreditation | 1 |
| CA-7 | Continuous Monitoring | 1 |
| CM-1 | Configuration Management Policy & Procedures | 1 |
| CM-2 | Baseline Configuration | 1 |
| CM-3 | Configuration Change Control | 1 |
| CM-4 | Security Impact Analysis | 1 |
| CM-5 | Access Restrictions for Change | 1 |
| CM-6 | Configuration Settings | 1 |
| CM-7 | Least functionality | 1 |
| CM-8 | Information System Component Inventory | 1 |
| CM-9 | Configuration Management Plan | 1 |

| Control | Control Name | Number of Systems Tested |
|---|---|---|
| CM-10 | Software Usage Restrictions | 1 |
| CM-11 | User-Installed Software | 1 |
| CP-1 | Contingency Planning Policy & Procedures | 1 |
| CP-2 | Contingency Plan | 1 |
| CP-4 | Contingency Plan Testing and Exercises | 1 |
| CP-6 | Alternate Storage Sites | 1 |
| CP-7 | Alternate Processing Sites | 1 |
| CP-8 | Telecommunication Services | 1 |
| CP-9 | Information System Backup | 1 |
| CP-10 | Information System Recovery & Reconstitution | 1 |
| IA-1 | Identification & Authentication Policy and Procedures | 1 |
| IA-2 | User Identification & Authentication (Organizational Users) | 1 |
| IA-3 | Device Identification & Authentication | 1 |
| IA-4 | Identifier Management | 1 |
| IA-5 | Authentication Management | 1 |
| IR-1 | Incident Response Policy & Procedures | 1 |
| IR-2 | Incident Response Training | 1 |
| IR-3 | Incident Response Testing | 1 |
| IR-4 | Incident Handling | 1 |
| IR-5 | Incident Monitoring | 1 |
| IR-6 | Incident Reporting | 1 |
| IR-8 | Incident Response Plan | 1 |
| PL-1 | Security Planning Policy & Procedures | 1 |
| PL-2 | System Security Plan | 1 |
| PL-4 | Rules of Behavior | 1 |
| PL-8 | Information Security Architecture | 1 |
| PS-1 | Personnel Security Policy & Procedures | 1 |
| PS-6 | Access Agreements | 1 |
| RA-1 | Risk Assessment Policy and Procedures | 1 |
| RA-2 | Security Categorization | 3 |
| RA-3 | Risk Assessment | 3 |
| RA-5 | Vulnerability Scanning | 1 |
| SA-1 | System & Services Acquisition Policy and Procedures | 1 |
| SA-3 | System Development Life Cycle Support | 1 |
| SA-4 | Acquisitions Process | 1 |
| SA-5 | Information System Documentation | 1 |

| Control | Control Name | Number of Systems Tested |
|---|---|---|
| SA-9 | External Information System Services | 3 |
| SC-7 | Boundary Protection | 1 |
| SC-8 | Transmission Confidentiality and Integrity | 1 |
| SI-2 | Flaw remediation | 1 |
| SI-4 | Information System Monitoring | 1 |
| SI-7 | Software, Firmware, and Information Integrity | 1 |
| PM-1 | Information Security Program Plan | 1 |
| PM-3 | Information Security Resources | 1 |
| PM-4 | Plan Of Action And Milestones Process | 1 |
| PM-5 | Information System Inventory | 1 |
| PM-6 | Information Security Measures Of Performance | 1 |
| PM-7 | Enterprise Architecture | 1 |
| PM-8 | Critical Infrastructure Plan | 1 |
| PM-9 | Risk Management Strategy | 1 |
| PM-10 | Security Authorization Process | 1 |
| PM-12 | Insider Threat Program | 1 |
| AR-5 | Privacy Awareness and Training | 1 |