Office of Inspector General

AUG 12 2016

The Honorable Robert N. Kaplan
President and Chief Executive Officer
Inter-American Foundation
1331 Pennsylvania Avenue NW
Suite 1200 North
Washington, DC 20004

Dear Mr. Kaplan:

The Cybersecurity Act of 2015, Public Law 114-113, Section 406 requires the inspector general of every agency that operates a Federal national security system or a Federal system that provides access to personally identifiable information (PII) to report the following information on the computer systems' security controls and practices:

- A description of the logical access policies and practices the agency uses to access a covered system, including whether appropriate standards were followed.

- A description and list of the logical access controls and multifactor authentication the agency uses to govern privileged users' access to covered systems.

- If the agency does not use logical access controls or multifactor authentication to access a covered system, the reasons why it does not use them.

- A description of the agency's information security management practices for the covered systems.

- A description of the agency's policies and procedures to ensure that entities providing services to the agency, including contractors, implement the information security management practices.

The U.S. Agency for International Development Office of Inspector General's (OIG) report on Inter-American Foundation's (IAF) information systems is enclosed. While IAF does not operate a national security system as described in Section 406, it does operate systems with access to PII. The independent certified public accounting firm CliftonLarsonAllen LLP prepared this report drawing on fieldwork it performed during its audit of IAF's fiscal year 2016 Federal Information Security Modernization Act (FISMA) compliance. Any deficiencies related to IAF's logical access policies, practices, or controls will be included in OIG's audit report on FISMA compliance later this year.

If you have any questions about our work, please contact me directly, or members of your staff may contact our congressional affairs office at 202-712-1150.

Sincerely,

/s/
Ann Calvaresi Barr
Inspector General

Enclosure

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.claconnect.com

August 9, 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:

The USAID Office of Inspector General tasked CliftonLarsonAllen LLP to assist in meeting its requirements to respond to Section 406(b)(2) of the CyberSecurity Act of 2015 for the Inter-American Foundation (IAF). Enclosed are our final responses.

In addressing the requirements, we leveraged the audit procedures performed during our current audit of IAF's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). To address requirements that were not reviewed as part of the FISMA audit, we assessed additional controls identified in National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

The attached final responses do not provide any conclusions or recommendations. Our overall conclusions and recommendations will be noted in the IAF FISMA audit report for fiscal year 2016.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

Final Response to Section 406(b)(2) of the Cybersecurity Act of 2015

The following presents responses to Section 406(b)(2) of the Cybersecurity Act of 2015 for the Inter-American Foundations (IAF) for the following selected systems: the Enterprise Network and the Grants Evaluation and Management System and one contractor system, Google Mail.

CyberSecurity Act of 2015 - Inspector General Reports On Covered Systems
Excerpt from Section 406(b):

(2) CONTENTS - The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

Response:
IAF has documented logical access policies and practices in the *IAF Information System Security Program,* dated May 28, 2015, and the *Enterprise Network System Security Program*, dated February 2016. The access control policies and practices cover procedures related to user access processes for establishing, modifying, and reviewing system accounts. In addition, the policies include procedures related to segregation of duties, remote access, least privilege, and access enforcement.

IAF requires all users to have an approved user access request form, signed rules of behavior, and completed security awareness training prior to being granted system access. Users are also only granted the permissions which were requested on their access request form. User accounts are reviewed for inactivity and disabled after 90 days of inactivity. In addition, user accounts are reviewed on an annual basis. Terminated/separated user accounts are disabled upon personnel termination.

IAF configures all accounts with the concept of segregation of duties and least privilege in mind. To gain privileged access to the network, the user must fill out the privileged access request form and have it reviewed and approved by the Chief Information Security Officer and sign the network administrator rules of behavior. IAF has a limited number of individuals with system administrator access. IAF also requires administrators to use different credentials to perform their administrative tasks.

IAF has configured their workstations to lock out user accounts after 5 invalid login attempts for a duration of 15 minutes to reduce the likelihood of unauthorized access to the network. IAF users are all granted the ability to connect to the Enterprise Network remotely. Users are required to use Symantec Validation & ID Protection for multi-factor authentication to remotely connect to the network.

To gain access to the Grants Evaluation and Management System (GEMS), users must have the specific GEMS access requested on the network access request form and sign the GEMS rules of behavior. GEMS accounts are monitored and manually disabled after 90 days of inactivity. Based on the testing completed, one account was identified with an active account after not being used for over 90 days. IAF noted that certain users only require access periodically for reporting purposes and has documented a list of personnel who are exempt from having their accounts disabled. The account that was identified was on the list of exempt accounts.

IAF has documented a segregation of duties matrix for the GEMS application which is checked when a new user account is created to ensure the permissions assigned to the account do not pose any segregation of duties conflicts. GEMS user accounts are also configured with the principle of least privilege and grant the most restrictive set of permissions necessary for the user to complete their job responsibilities.

Access to Google Mail is granted as part of the on boarding and network access processes. There are no automated controls to automatically disable Google Mail accounts after the 90 day inactivity period is reached. If a user account is disabled for inactivity, a member of the administrator staff disables the Google Mail account. When a user is terminated, IAF disables the account until the e-mail can be backed up to the IAF file server. Once the terminated user's email is backed up, the Google Mail account is deleted. IAF has two administrators of Google Mail and the rest of the users are non-privileged users. Google Mail can be accessed remotely and requires multi-factor authentication.

Based on the testing completed, IAF is following the access controls procedures.

(B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

Response:
IAF currently has logical access controls in place for privileged users. IAF requires privileged users to have two domain accounts. One is their normal user account for their day to day activities. The second is an elevated privilege account which they use to perform actions requiring administrative access. To be granted access to a privileged account the user must fill out an administrative privileges request form which is reviewed and approved by the Chief Information Security Officer.

Multi-factor authentication for privileged users is currently not implemented.

(C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

Response:
Multi-factor authentication for privileged and non-privileged users is currently not implemented. Management indicated that currently it is not feasible to implement multi-factor authentication for privileged users. IAF has purchased equipment capable of accepting Personal Identity Verification cards so IAF will be ready to use Personal Identity Verification cards when it becomes more cost effective and feasible to implement.

(D) A description of the following information security management practices used by the covered agency regarding covered systems:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

Response:
IAF does not have a formally documented policy on conducting inventories and also does not have an automated process for conducting inventories of software on the IAF network. IAF has a practice of purchasing 60 licenses for any software procured because the historical data shows they have never needed more than 55 licenses. IAF manually tracks the contracts for the licenses for renewal. The tracking spreadsheet is updated annually or when new software is purchased.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including-(I) data loss prevention capabilities; (II) forensics and visibility capabilities; or (III) digital rights management capabilities.

Response:
For data loss prevention, IAF did not have any data loss prevention mechanisms in place.

Regarding forensic and visibility capabilities, IAF has a contractor who is responsible for vulnerability scanning and analysis and will perform forensic analysis when necessary. IAF has not performed any forensic analysis because there have not been any incidents in the past 3 years requiring forensic analysis.

IAF does not have a formally documented policy on conducting inventories and also does not have an automated process for conducting inventories of software on the IAF network. For digital rights management, IAF manually tracks licenses as noted in clause (i).

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

Response:
For data loss prevention, IAF did not have any data loss prevention mechanisms in place. IAF did however note that they use a combination of tools to discourage, reduce, and prevent data loss prevention across the organization, which included the following:

- IAF encrypts all backup tapes that go offsite for vault storage.
- IAF has check point full disk encryption for all mobile government furnished equipment.
- IAF web traffic and browser based transactions all use HTTPS for items like invoice payments, agency financial report access, personal government file review, procurement creations, etc.
- IAF specific web transactions are controlled by a whitelist for the IAF Network and a correlating user account on the external system.
- IAF uses Zixmail for encrypting sensitive data sent via email.
- IAF also uses P2P IPSEC firewall connections for specific Human Resource functions between IAF and Interior Business Center.
- IAF does not furnish any DVD's or USB's for government use and IAF has informed users to not copy government data to external sources.

Regarding forensic and visibility capabilities, IAF has a contractor who is responsible for vulnerability scanning and analysis. The contractor has access to a wide suite of tools to research and analyze incidents on the network. IAF also reports incidents to United States Computer Emergency Readiness Team for further analysis, if necessary.

For digital rights management, IAF does not have a formally documented policy on conducting inventories and also does not have an automated process for conducting inventories of software on the IAF network. IAF has a practice of purchasing 60 licenses for any software procured because the historical data shows they have never needed more than 55 licenses. IAF manually tracks the contracts for the licenses for renewal. The tracking spreadsheet is updated annually or when new software is purchased.

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

Response:
IAF management stated that implementing data loss prevention is not feasible to implement because of the high cost associated with implementation. IAF also noted it would hinder the users' ability to complete their work. IAF is planning on implementing the Google Mail data loss prevention once it is available.

IAF was not actively using the contractor's capability to perform forensic investigations because IAF has not had an incident requiring forensic investigation in the past 3 years.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

Response:
IAF has documented policies and procedures in the *IAF Information System Security Program,* dated May 28, 2015, to ensure that external entities have the required security controls. IAF requires all connections from the IAF Enterprise Network to an information system outside of the system authorization boundary be documented with an Interconnection Security Agreement. The Interconnection Security Agreement documents the interface characteristics, security requirements and which party is responsible for which security requirements, and the nature of information communicated through the connection. The Chief Information Officer reviews the Interconnection Security Agreements annually to ensure the security requirements are being appropriately maintained. Based on testing completed, the Memorandum of Understand/Interconnection Security Agreement between IAF and another agency expired on January 17, 2016. IAF submitted the Interconnection Security Agreement to the agency; however, it had not provided a current signed agreement.