Office of Inspector General

AUG 12 2015

The Honorable Elizabeth Littlefield
President and Chief Executive Officer
Overseas Private Investment Corporation
1100 New York Avenue NW
12th Floor
Washington, DC 20527

Dear Ms. Littlefield:

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 the Overseas Private Investment Corporation's (OPIC) information systems is enclosed. While OPIC 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 OPIC's fiscal year 2016 Federal Information Security Modernization Act (FISMA)

compliance. Any deficiencies related to OPIC's logical access policies, practices, or controls will be included in OIG's audit report on FISMA compliance later this year.

We have redacted sensitive but unclassified information pertaining to USADF's information security practices from the attached responses pursuant to Freedom of Information Act exemption 7(E), 5 U.S.C. § 552(b)(7)(E).

If you have any questions about our work, please contact me directly, or members of your staff may contact our Assistant Inspector General for Audit, Thomas Yatsco at 202-712-1150.

Sincerely,

/s/
Ann Calvaresi Barr
Inspector General

Enclosure

CliftonLarsonAllen LLP
11710 Beltsville Drive, Suite 300
Calverton, Maryland 20705
301-931-2050 fax 301-931-1710
www.claconnect.com

August 12, 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 Overseas Private Investment Corporation (OPIC). Enclosed are our responses.

In addressing the requirements, we leveraged the audit procedures performed during our current audit of OPIC'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 responses do not provide any conclusions or recommendations. Our overall conclusions and recommendations will be noted in the OPIC 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

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 Overseas Private Investment Corporation (OPIC) for the selected covered system, OPIC Network.

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:
OPIC has documented logical access policies and procedures and has implemented the procedures for the covered systems. *OPIC Access Control Procedure* dated April 6, 2015, describes the process of how users are granted access, how access is modified, and how access is removed as well as procedures related to segregation of duties, least privilege, session lock, remote access, and controls over mobile devices.

(~~SBU~~) OPIC manages logical access to the system through [redacted], which is a [redacted] used to document the requests for new user access as well as [redacted] requests. Once the request is approved, the operations team begins to build the account to the specifications outlined in the request. Users are also required to take security awareness training and rules of behavior training. OPIC tracks the completion of the trainings through its [redacted]. User accounts are [redacted]; however, the [redacted]. User accounts that have been [redacted] are reviewed by the operations staff and they determine whether the accounts should be [redacted]. OPIC enforces access to the system by only granting access to users that were approved on a [redacted]. OPIC also reviews all access requests to ensure the new access will not conflict with their current level of access. OPIC has a policy to give users the least access required to complete their jobs. OPIC performs an [redacted] of its user and [redacted]. OPIC is working to implement a process which incorporates [redacted] review.

(~~SBU~~) OPIC has configured their workstations to [redacted] to reduce the likelihood of unauthorized access to the network. To gain [redacted] to the network users are required to complete the rules of behavior training and [redacted].

(~~SBU~~) Based on testing completed, OPIC is following the access control procedures for the OPIC Network except in regards to [redacted] accounts.

(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:
(~~SBU~~) OPIC currently has logical access controls in place for [redacted]. OPIC requires [redacted] to have an approved [redacted] request form before being granted [redacted]. [redacted] are required to log in with their [redacted].

(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:
(~~SBU~~) OPIC did not implement [redacted] because Office of Management and Budget's (OMB) implementation of Homeland Security Presidential Directive 12 did not apply to government corporations. However, this was revised in OMB memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government.* That memorandum [redacted]. OPIC management is investigating the corporation's capability to implement [redacted].

(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:
(~~SBU~~) OPIC defines its requirements for tracking licenses in the *OPIC Information System Security Policy*, dated February 22, 2016. OPIC uses [redacted] and [redacted] to enumerate software installed on OPIC Network workstations and servers. Licensed software is tracked [redacted] for review at any time by the Chief Information Officer/Chief Information Security Officer staff. The [redacted] repository automatically sends renewal notifications to OPIC management 45 days before licenses expire.

(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:
(~~SBU~~) For data loss prevention, OPIC uses the data loss prevention methods [redacted].

(~~SBU~~) Regarding forensic capabilities, OPIC's *Incident Handling and Response Procedure* dated May 2015, includes procedures for identifying a suspicious event and conducting an investigation. OPIC has [redacted] that will review suspicious events on the network and leverage prior investigations as well as software tools to monitor for and investigate incidents.

For digital rights management, OPIC has the capability to conduct automated inventories of the software on the OPIC Network.

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

Response:
(~~SBU~~) For data loss prevention, OPIC uses [redacted] to monitor the network and determine whether there are rouge hosts or OPIC employees that are exfiltrating data. If exfiltration is detected, OPIC staff will [redacted] and begin an investigation into the source of the connection.

(~~SBU~~) Regarding forensic capability, OPIC's *Incident Handling and Response Procedure* dated May 2015, discusses procedures for identifying a suspicious event and conducting an investigation. OPIC has [redacted] research suspicious activity. Once the OPIC team has positively identified an incident requiring forensic analysis, the team will leverage [redacted] to perform forensic investigations. The investigations result from indicators of compromise on an OPIC asset. Using the indicators of compromise, OPIC also correlates the newly identified incident with past incidents to look for patterns and help speed up the analysis process.

(~~SBU~~) For digital rights management, OPIC uses [redacted] to enumerate software installed on the OPIC Network workstations and servers. Licensed software is tracked [redacted] for review at any time by the Chief Information Officer/Chief Information Security Officer staff. The [redacted] software repository sends automated renewal notifications to OPIC management 45 days before licenses expire.

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

Response:
Not applicable. OPIC is using capabilities described in clause (ii).

(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:
(~~SBU~~) OPIC has policies and procedures in place requiring entities, including contractors that provide services to OPIC, to implement security management

practices. OPIC's *Assessment and Authorization Procedures* requires non-OPIC systems that are connected to OPIC Network to have an interconnection security agreement. The agreement identifies what security controls are required to be in place and which party is responsible for implementing the required security controls. In addition, OPIC uses other contractor systems, such as [redacted], that do not have a dedicated connection between the information systems and OPIC. OPIC has access to the [redacted] associated security documentation, such as the system security plan, risk assessment, and security assessment report. [redacted] is a FedRAMP compliant Software as a Service information system with an authorization to operation dated November 13, 2014.

OPIC requires all contractors to have a position risk designation performed using the Office of Personnel Management Position Designation Automated Tool. The Contract Officer's Representative will answer a questionnaire about the potential risks for the position. As a result, the tool will identify the level of background check necessary for the specified position. The OPIC Security Officer will then initiate the background check identified by the tool for the contractor. All personnel, including contractors or others working on behalf of OPIC, accessing OPIC systems are required to complete initial security awareness training and annual refresher training. In addition, contractors with system access must comply with same access control procedure noted in Section A.