



**OFFICE OF INSPECTOR GENERAL**  
Overseas Private Investment Corporation

**OPIC Implemented  
Controls in Support of  
FISMA for Fiscal Year 2017  
but Improvements Are  
Needed**

**AUDIT REPORT A-OPC-17-007-C**  
**SEPTEMBER 28, 2017**

1300 Pennsylvania Avenue NW • Washington, DC 20523  
[oig.usaid.gov](http://oig.usaid.gov) • 202-712-1150

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**

### **Overseas Private Investment Corporation Hotline**

Email: [opichotline@usaid.gov](mailto:opichotline@usaid.gov)

Phone: 202-712-1023 or 800-230-6539

Mail: USAID OIG Hotline, Attn: OPIC Hotline, P.O. Box 657, Washington, DC 20044-0657



## MEMORANDUM

**DATE:** September 28, 2017

**TO:** OPIC, Vice President, Michele Perez

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

**SUBJECT:** OPIC Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed (A-OPC-17-007-C)

Enclosed is the final audit report on the Overseas Private Investment Corporation's (OPIC) 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 of 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 OPIC'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 OPIC implemented certain security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested OPIC'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 auditors reviewed each of the six systems in OPIC's inventory. Fieldwork took place at OPIC's headquarters in Washington, DC, from February 15 to July 7, 2017.

Clifton concluded that OPIC implemented 98 of 104 selected security controls that were designed to preserve the confidentiality, integrity, and availability of its information and information systems. For example, OPIC did the following:

- Effectively monitored, reviewed, and analyzed audit logs.
- Categorized its information systems and the information processed, stored or transmitted on them in accordance with Federal guidelines.
- Designated senior officials in the organization to review and approve the security categorizations.
- Implemented system and service acquisition controls.
- Implemented change management policy and procedures.
- Implemented an effective program for responding to and handling incidents.
- Maintained an adequate and effective training program for general, specialized, and privileged users.
- Maintained an effective process to review inactive and separated users across the tested systems.
- Implemented multifactor authentication for remote access.

However, the auditors found OPIC did not effectively implement 6 of 104 controls. To address the weaknesses identified, Clifton made and OIG agrees with the following recommendations to OPIC's management, which we will track until they are fully implemented. We recommend OPIC's chief information officer:

**Recommendation 1.** Remediate network vulnerabilities identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.

**Recommendation 2.** Prepare a written authorization to operate each application or service, or decommission them and document the results.

**Recommendation 3.** Document and implement an automated process to track the annual reviews of the Information Security Program Plan and update it, if needed.

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

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



**The Overseas Private Investment Corporation Has Implemented  
Many Controls in Support of FISMA, However Improvements Are  
Needed**

**Fiscal Year 2017**

CliftonLarsonAllen LLP  
901 N. Glebe Road, Suite 200  
Arlington, VA 22203  
571-227-9500 | fax 571-227-9552  
[CLAconnect.com](http://CLAconnect.com)



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

September 20, 2017

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 Overseas Private Investment Corporation's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The Overseas Private Investment Corporation Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed*. The USAID Office of Inspector General 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 OPIC's information security program.

The objective of this performance audit was to determine whether OPIC implemented certain 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 selected controls from all six of OPIC's systems included in the system inventory as of October 15, 2016. The audit also included a vulnerability assessment of OPIC's general support system and an evaluation of OPIC's process for identifying and correcting/mitigating technical vulnerabilities. Audit fieldwork was performed at OPIC's headquarters in Washington, D.C., from February 15, 2017, to July 27, 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 OPIC generally complied with FISMA requirements by implementing many selected security controls for selected information systems. Although OPIC 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 corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in OPIC's information security program that needed to be improved. We are

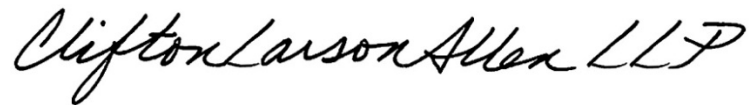
making three recommendations to assist OPIC in strengthening its information security program. In addition, findings related to four recommendations from prior years were not yet fully implemented and therefore new recommendations were not made.

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

Very truly yours,

CLIFTONLARSONALLEN LLP

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style with a large initial 'C' and 'L'.

# TABLE OF CONTENTS

<b>Summary of Results</b> .....	1
<b>Audit Findings</b> .....	4
Security Controls Surrounding Patch and Configuration Management Need to be Strengthened .....	4
Network Accounts Need to be Periodically Reviewed .....	5
Certain Authentication Requirements Need to be Fully Met.....	5
Asset Management Controls Need to be Strengthened.....	6
Enterprise Architecture Controls Need to be Strengthened .....	6
Components of OPIC's System Inventory Need to be Fully Assessed.....	7
OPIC's Information Security Program Plan Needs to be Updated .....	8
<b>Evaluation of Management Comments</b> .....	10
<b>Appendix I – Scope and Methodology</b> .....	11
<b>Appendix II – Management Comments</b> .....	13
<b>Appendix II – Number of Controls Reviewed for Each System</b> .....	15



# SUMMARY OF RESULTS

The Federal Information Security Modernization Act of 2014<sup>1</sup> (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 sources. Because the Overseas Private Investment Corporation (OPIC) 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 United States Agency for International Development's Office of Inspector General engaged CliftonLarsonAllen LLP to conduct an audit in support of the FISMA requirement for an annual evaluation of OPIC's information security program. The objective of this performance audit was to determine whether OPIC implemented certain security controls for selected information systems 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 all six of OPIC's systems<sup>2</sup> included in its system inventory as of October 15, 2016.

## Results

The audit concluded that OPIC implemented 98 of 104 security controls for its information systems in support of FISMA. For example, OPIC:

- Implemented effective audit log monitoring, review and analysis.

---

<sup>1</sup> The Federal Information Security Modernization Act of 2014 amends the FISMA Act of 2002 to (1) reestablish the oversight authority of the Director of the Office of Management and Budget with respect to agency information security policies and practices and (2) set forth authority for the Secretary of Homeland Security to administer the implementation of such policies and practices for information systems.

<sup>2</sup> Systems include major applications and general support systems as defined by the Office of Management and Budget Circular A-130, Appendix III.

- Categorized its information systems and the information processed, stored or transmitted in accordance with federal guidelines, and designated senior-level officials within the organization to review and approve the security categorizations.
- Implemented system and service acquisition controls.
- Implemented change management policy and procedures.
- Implemented an effective program for incident handling and response.
- Maintained an effective training program for general, specialized, and privileged users.
- Maintained an effective process for reviewing inactive and separated users across the tested systems.
- Implemented multifactor authentication for remote access.

Although OPIC had policies for its information security program, its implementation of those policies was not always fully effective to preserve the confidentiality, integrity, and availability of the corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. The audit found that OPIC had not effectively implemented 6 of 104 controls selected for testing and identified the following actions that OPIC needed to take to correct the weaknesses in its information security program:

- Security controls surrounding patch and configuration management need to be strengthened.
- Network accounts need to be periodically reviewed.
- Certain authentication requirements need to be fully met.
- Asset management controls need to be strengthened.
- Enterprise architecture controls need to be strengthened.
- Components of OPIC's system inventory need to be fully assessed.<sup>3</sup>
- OPIC's Information Security Program Plan needs to be updated.

---

<sup>3</sup> The control related to this finding was not selected for review among the 104 controls. However, this finding was identified when we assessed OPIC's actions taken in response to Recommendation 16 in *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016). Therefore, we are reporting our finding in this report.

We have made three recommendations to assist OPIC in strengthening its information security program. In addition, four recommendations from prior years were not fully implemented and therefore new recommendations were not made. Based on our evaluation of management comments, we acknowledge management decisions on all recommendations. OPIC's comments are included in their entirety in Appendix II.

Detailed findings appear in the following section.

# AUDIT FINDINGS

## 1. Security Controls Surrounding Patch and Configuration Management Need to be Strengthened

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 organization:

\* \* \*

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

Independent scans performed using the software tool Nessus noted vulnerabilities on one of OPIC's systems based on Common Vulnerabilities and Exposures<sup>4</sup> identification.

Although OPIC identified similar vulnerabilities during the corporation's scanning process, their scans had the "do not show superseded patches" option enabled. This option allows Tenable's Security Center to only report the most recent patch which will fix a vulnerability. While this is useful for OPIC's remediation team, it does not show the full scope of how many vulnerabilities exist on the network.

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

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Corporation employees may be unable to access systems.
- Corporation data may be lost, stolen or used for nefarious means.

As a result, we recommend the following.

***Recommendation 1:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer remediate vulnerabilities on the network identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.*

---

<sup>4</sup> Common Vulnerabilities and Exposures is a dictionary of common names for publicly known IT system vulnerabilities. (Source: NIST Special Publication 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme).

## 2. Network Accounts Need to be Periodically Reviewed

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

The organization manages information system accounts, including:

\* \* \*

h. Notifies account managers:

1. When accounts are no longer required.

\* \* \*

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency].

In fiscal year 2017, OPIC established a documented process for reviewing service accounts; however, the process had not been fully implemented. Thus, 4 of 15 sampled service accounts were not recertified on an annual basis. OPIC management indicated that the team performing the recertification was continuing to work through the accounts; however, a complete recertification of the accounts had not been completed. By not performing periodic recertification, there is an increased risk of unauthorized privileged access to critical systems.

A recommendation addressing this finding was issued in the fiscal year 2015 FISMA audit.<sup>5</sup> At the end of audit fieldwork in fiscal year 2016, OPIC documented its process for reviewing service accounts. However, the process had not been fully implemented as of June 2017 and the recommendation remains open. Therefore, we are not making an additional recommendation at this time.

## 3. Certain Authentication Requirements Need to be Fully Met

NIST Special Publication 800-53, Revision 4, and other guidance, describe circumstances in which an organization must implement authentication.

However, OPIC did not fully meet authentication requirements because certain requirements did not become effective for the corporation until October 30, 2015. According to OPIC management, they plan to finish implementing the requirements by September 30, 2017. Nonetheless, by not fully meeting certain authentication requirements, OPIC increased the risk of compromising the confidentiality and integrity of the corporation's information.

A recommendation addressing this finding was issued in the fiscal year 2016 audit.<sup>6</sup> Therefore, we are not making a new recommendation at this time.

---

<sup>5</sup> Recommendation 1, *Audit of the Overseas Private Investment Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, as Amended* (Audit Report No. A-OPC-15-0009-P, September 17, 2015).

<sup>6</sup> Recommendation 5, *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016).

## 4. Asset Management Controls Need to be Strengthened

NIST Special Publication 800-53, Revision 4, security control CM-8, states the following regarding Information System Component Inventory:

The organization:

- b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Control Enhancements:

- 1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

OPIC had not completed wall-to-wall inventories on a quarterly basis as defined in its *Information System Security Policy* and the OPIC 800-53 parameter requirements.<sup>7</sup> Due to competing priorities, OPIC management indicated that they had not been able to dedicate the time and resources necessary to complete a full asset inventory.

Without maintaining an updated component inventory, OPIC is more susceptible to lost or misplaced assets that may result in unauthorized access to OPIC data.

A recommendation addressing this finding was issued in the fiscal year 2016 audit.<sup>8</sup> OPIC plans to take final corrective action by the end of fiscal year 2017. Therefore, we are not making a new recommendation at this time.

## 5. Enterprise Architecture Controls Need to be Strengthened

NIST Special Publication 800-53, Revision 4, security control PM-7, states the following regarding enterprise architecture:

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

NIST Special Publication (SP) 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the Risk Management Framework to Federal information systems including the alignment of security controls the enterprise<sup>9</sup> and security architecture.

---

<sup>7</sup> *Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters* (May 20, 2015).

<sup>8</sup> Recommendation 7, *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016).

<sup>9</sup> Federal Enterprise Architecture Reference Models and Segment and Solution Architectures are defined in the OMB Federal Enterprise Architecture (FEA) Program, FEA Consolidated Reference Model Document, Version 2.3, October 2003 and OMB Federal Segment Architecture Methodology (FSAM), January 2009, respectively.

During fiscal year 2016, OPIC did not have enterprise architecture policies or procedures documented. OPIC had a risk management committee and strategy; however, management had not formally documented the enterprise architecture strategy to reduce associated risks to information security. In addition, management indicated that they did not have personnel assigned to document and implement an enterprise architecture strategy.

During our fiscal year 2017 fieldwork, OPIC still did not have documented enterprise architecture policies or procedures. OPIC was working towards developing an enterprise architecture in line with the Federal Enterprise Architecture and Risk Management Framework. OPIC management indicated an expected completion date of September 30, 2017.

The lack of risk management controls for enterprise architecture may increase the difficulty the corporation has with managing the integration of security for its IT projects and assets.

A recommendation addressing this finding was issued in the fiscal year 2016 audit.<sup>10</sup> Because OPIC management had not taken final corrective action, we are not making an additional recommendation at this time.

## **6. Components of OPIC's System Inventory Need to be Fully Assessed**

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

The organization:

- a. Assigns a senior-level executive or manager as the authorizing official for the information system;
- b. Ensures that the authorizing official authorizes the information system for processing before commencing operations.

NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, states the following regarding system boundaries and major applications:

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific, mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel).

---

<sup>10</sup> Recommendation 10, *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016).

In fiscal year 2016, one system had an authorization boundary of all external services. However, that system consisted of four individual portfolio mission functions, rather than a single mission function.

In addition, although the four portfolios in that system had individual authorizations to operate (ATOs), the individual services contained expired external ATOs, outdated information, and incomplete plans of action and milestones.

During our fiscal year 2017 fieldwork, OPIC management removed the system as a FISMA reportable system. Each service previously covered under the ATO was being reevaluated to determine whether the service would be classified as a minor application or have its own assessment and authorization completed. However, due to the large number of services covered by the previous ATO, OPIC had not completed the evaluations. OPIC plans to complete the evaluation by September 30, 2017.

Without adequately segmenting system ownership and maintaining accurate external system security statuses, parties may not be aware of their responsibilities to enable them to make informed decisions regarding system risks. Therefore, we are making the following recommendation.

***Recommendation 2:*** *We recommend that the Overseas Private Investment Corporation's Vice President, Department of Management and Administration, either prepare a written authorization to operate or decommission each external application or service and document the results.*

## **7. OPIC's Information Security Program Plan Needs to be Updated**

NIST Special Publication 800-53, Revision 4, security control PM-1, states the following regarding an Information Security Program Plan:

The organization:

- b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*];
- c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.

In addition, the *Overseas Private Investment Corporation Network System Security Plan (SSP)*, states the following regarding (PM-1):

ISPP is reviewed annually and updated as necessary based on organizational changes.

However, OPIC's *Information Security Program Plan (ISPP)* was not up-to-date. This occurred because management was relying on a manual process to track and update policies and procedures. Management indicated they are working towards implementing a process to automate scheduled reviews and updates to policies and procedures.



As a result of this weakness, the policy may no longer reflect OPIC's current environment. Therefore, we are making the following recommendation.

***Recommendation 3:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement an automated process to track the annual reviews of the Information Security Program Plan and update it, if needed.*

# EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Overseas Private Investment Corporation (OPIC) described planned actions to address all three recommendations. OPIC'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. 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 OPIC implemented certain security controls for selected information systems 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, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4*. We assessed OPIC's performance and compliance with FISMA in the following areas:

- Access Controls
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition

For this audit, we reviewed selected controls from all six of OPIC's systems included in the system inventory as of October 15, 2016. See Appendix II for a listing of selected controls. The audit also included a vulnerability assessment of one of OPIC's systems and an evaluation of OPIC's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit recommendations<sup>11</sup> to determine if OPIC had made progress in implementing the recommended improvements concerning its information security program.

---

<sup>11</sup> *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016).

The audit fieldwork was performed at OPIC's headquarters in Washington, D.C., from February 15, 2017, to July 27, 2017.

## Methodology

To determine if OPIC's information security program met FISMA requirements, we conducted interviews with OPIC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, OPIC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) identification and authentication policies and procedures; and (5) change control documentation. Where appropriate, we compared documents, such as the IT policies and procedures, to requirements stipulated in National Institute of Standards and Technology special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, we completed a vulnerability assessment of one of OPIC's systems and evaluated OPIC's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of OPIC's vulnerability scanning configurations and network vulnerability scanning results and comparing them with our independent network vulnerability scanning results. We also reviewed the status of the audit recommendations in the fiscal year 2016 FISMA audit report.<sup>12</sup>

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.

---

<sup>12</sup> *The Overseas Private Investment Corporation Has Implemented Many Controls In Support of FISMA For Fiscal Year 2016, But Improvements Are Needed* (Audit Report No. A-OPC-17-005-C, November 7, 2016).

# Management Comments



MEMORANDUM

September 13, 2017

TO: Alvin Brown  
Deputy Assistant Inspector General  
USAID – Office of the Inspector General

FROM: Michele Perez  
Vice President, Department of Management and Administration  
Overseas Private Investment Corporation (OPIC)

SUBJECT: OPIC Comments on the Audit of the Overseas Private Investment Corporation’s Fiscal Year 2017 Compliance with Provisions of the Federal Information Security Modernization Act of 2014

Below is the Overseas Private Investment Corporation’s response to the Office of Inspector General’s (OIG) DRAFT report “*OPIC has Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements are Needed (A-OPC-17-00X-C).*”

The Inspector General report contains 3 recommendations for corrective action. This memorandum provides OPIC’s management responses to these recommendations. The Federal Information Security Modernization Act of 2014 (FISMA) and the NIST Risk Management Framework defined in NIST Special Publication 800-37 are the foundation of OPIC’s information system security program. As indicated in the report, OPIC’s program successfully implemented over 94% (98/104) of the security controls tested.

**Recommendation No. 1:** We recommend that the Overseas Private Investment Corporation’s Chief Information Officer remediate network vulnerabilities identified by the Office of Inspector General, as appropriate, or document acceptance of the risks of those vulnerabilities.

**Management Response:** OPIC values the Inspector General’s acknowledgment that our vulnerability scanning system identified the same vulnerabilities as its contractor, even though our system did not record superseded patches. Of the identified known vulnerabilities, the Chief Information Officer will remediate those that may adversely impact OPIC systems. For those vulnerabilities that management chooses not to remediate, the Chief Information Officer will document OPIC’s risk acceptance **by May 31, 2018.**

**Recommendation No. 2:** We recommend that the Overseas Private Investment Corporation's Vice President, Department of Management and Administration, either prepare a written authorization to operate or decommission each external application or service and document the results.

**Management Response:** OPIC has established a schedule by which we are reviewing our external service providers and is currently following that schedule to ensure we review all external service provider systems annually. We started this process in June of 2017, and the VP DMA, in consultation with the CIO, will ensure completion of this annual review of all external systems **by June 30, 2018**.

**Recommendation No. 3:** We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement an automated process to review and update the *Information Security Program Plan* on the corporation-defined basis.

**Management Response:** The Chief Information Officer will document and implement an automated process to review and update the Information Security Program Plan on the corporate-defined basis **by November 30, 2017**.

**/s/ Michele Perez**

# Number of Controls Reviewed for Each System

Control	Control Name	Number of Systems Tested
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	1
RA-3	Risk Assessment	1
RA-5	Vulnerability Scanning	1
PL-1	Security Planning Policy and Procedures	1
PL-2	System Security Plan	1
SA-1	System & Services Acquisition Policy and Procedures	1
SA-4	Acquisitions Process	1
SA-5	Information System Documentation	1
SA-9	External Information System Services	2
SA-10	Developer Configuration Management	1
SA-11	Developer Security Testing and Evaluation	1
PS-6	Access Agreements	1
CP-1	Contingency Planning Policy & Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	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
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
MA-1	System Maintenance Policy and Procedures	1
MA-2	Controlled Maintenance	1
MA-3	Maintenance Tools	1

<b>Control</b>	<b>Control Name</b>	<b>Number of Systems Tested</b>
MA-4	Nonlocal Maintenance	1
MA-5	Maintenance Personnel	1
MA-6	Timely Maintenance	1
SI-1	System & Information Integrity Policy and Procedures	1
SI-2	Flaw remediation	1
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-5	Security Alerts & Advisories	1
SI-7	Software and Information Integrity	1
SI-8	Spam Protection	1
SI-10	Information Input Validation	1
SI-11	Error Handling	1
SI-12	Information Output Handling and Retention	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
IR-5	Incident Monitoring	1
IR-6	Incident Reporting	1
IR-8	Incident Response Plan	1
AT-1	Security Awareness & Training Policy and Procedures	1
AT-2	Security Awareness	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
IA-1	Identification & Authentication Policy and Procedures	1
IA-2	Identification & Authentication (Organizational Users)	1
IA-3	Device Identification & Authentication	1
IA-4	Identifier Management	1
IA-5	Authenticator Management	1
AC-1	Access Control Policy & Procedures	1
AC-2	Account Management	3
AC-3	Access Enforcement	1
AC-4	Information Flow Enforcement	1
AC-5	Separation of Duties	3
AC-6	Least Privilege	1
AC-7	Unsuccessful Login Attempts	1
AC-8	System use Notification	1
AC-11	Session Lock	1
AC-17	Remote Access	1
AC-19	Access Control for Mobile Devices	1
AC-20	Use of External Information Systems	4
AU-6	Audit, Review, Analysis and Reporting	3



<b>Control</b>	<b>Control Name</b>	<b>Number of Systems Tested</b>
SC-1	System & Communications Protection Policy & Procedures	1
SC-2	Application Partitioning	1
SC-4	Information in Shared Resources	1
SC-5	Denial of Service Protection	1
SC-7	Boundary Protection	1
SC-8	Transmission Integrity	1
CA-1	Security Assessment and Authorization Policy & Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	1
CA-7	Continuous Monitoring	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