



OFFICE OF INSPECTOR GENERAL  
U.S. Agency for International Development

# OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018

**AUDIT REPORT A-OPC-19-006-C**  
**JANUARY 30, 2019**

1300 Pennsylvania Avenue NW • Washington, DC 20523  
<https://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**

### **USAID OIG Hotline**

Email: [ig.hotline@usaid.gov](mailto:ig.hotline@usaid.gov)

Complaint form: <https://oig.usaid.gov/complainant-select>

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

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



## MEMORANDUM

DATE: January 30, 2019

TO: Overseas Private Investment Corporation, Vice President, Michele Perez

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

SUBJECT: OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (A-OPC-19-006-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 2018. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown and Company CPAs and Management Consultants PLLC (Brown & Company) to conduct the audit. The contract required the audit firm to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Brown & Company's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit 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. Brown & Company is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which the audit firm did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether OPIC implemented selected security controls for certain information systems in support of FISMA. To answer the audit objective, Brown & Company evaluated OPIC's implementation 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." The audit firm reviewed selected controls from two OPIC-managed systems and four applications managed by external contractors. Fieldwork was performed at OPIC's headquarters in Washington, DC, from June 13 through October 4, 2018.

The audit firm concluded that OPIC generally complied with FISMA by implementing 65 of 72 security controls reviewed for the selected information systems. The controls are designed to

preserve the confidentiality, integrity, and availability of the Corporation's information and information systems. Among the controls OPIC implemented were the following:

- Audit log monitoring, review, and analysis.
- Categorization of its information systems and the information processed, stored, or transmitted in accordance with Federal guidelines, and designation of senior officials to review and approve the security categorizations.
- System and service acquisition controls.
- Change management policy and procedures.
- A program for incident handling and response.
- A training program for general, specialized, and privileged users.
- Multifactor authentication for remote access.

However, OPIC did not implement seven controls related to its privacy program, network vulnerabilities, account management, interconnection security agreements, and contingency planning.

To address the weaknesses identified in the report, we recommend that OPIC's chief information officer:

**Recommendation 1.** Document and implement a process to update its privacy impact assessments for the Corporation's information systems.

**Recommendation 2.** Remediate patch and configuration 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 3.** Document and implement a process to verify that patches are applied in a timely manner.

**Recommendation 4.** Document and implement a process to verify that (1) the account management system is updated promptly to support the management of information system accounts and (2) inactive accounts are promptly disabled after 30 days in accordance with the Corporation's access control procedures.

**Recommendation 5.** Document and implement procedures to record the date that system user accounts are disabled or deleted.

**Recommendation 6.** Document and implement a process to verify that interconnection security agreements and memorandums of understanding are annually reviewed and, if needed, updated.

**Recommendation 7.** Conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC's policy.

In finalizing the report, the audit firm evaluated OPIC's responses to the recommendations. After reviewing that evaluation, we consider recommendation 5 closed and recommendations 1 through 4, 6, and 7 resolved but open pending completion of planned activities. For recommendations 1 through 4, 6, and 7, please provide evidence of final action to [OIGAuditTracking@usaid.gov](mailto:OIGAuditTracking@usaid.gov).

We appreciate the assistance extended to our staff and Brown & Company's employees during the engagement.

# **The Overseas Private Investment Corporation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018**



## **Final Report December 11, 2018**

**Prepared by**

**Brown & Company CPAs and Management Consultants, PLLC  
1101 Mercantile Lane, Suite 122  
Largo, Maryland 20774**



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 our report on the Overseas Private Investment Corporation's (OPIC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The Overseas Private Investment Corporation Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018*. The USAID Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs 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 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 OPIC's six information systems. The audit also included a vulnerability assessment of OPIC's general support system and an evaluation of OPIC's process for identifying and mitigating information systems vulnerabilities. Audit fieldwork was performed at the Overseas Private Investment Corporation's headquarters in Washington, D.C., from June 13, 2018 through October 4, 2018.

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.

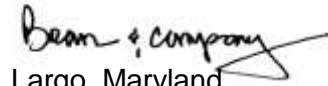
The audit concluded that OPIC generally complied with FISMA requirements by implementing many selected security controls for selected information systems. Although OPIC generally had policies for its information security program, its implementation of those policies for selected controls was not fully 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 seven recommendations to assist OPIC in strengthening its information security program. In addition, a finding related to one recommendation from a prior year was not yet fully implemented, and therefore, a new recommendation was 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.

Brown & Company CPAs and  
Management Consultants, PLLC



Largo, Maryland  
December 6, 2018



# TABLE OF CONTENTS

<b>Summary of Results .....</b>	<b>1</b>
<b>Audit Findings.....</b>	<b>3</b>
OPIC Needs to Update Its Privacy Impact Assessments.....	3
OPIC Needs to Mitigate Network Vulnerabilities.....	4
OPIC Needs to Improve Account Management Procedures.....	5
OPIC Needs to Review and Update Interconnection Security Agreements .....	7
OPIC Needs to Provide Contingency Training and Test the Contingency Plan .....	7
<b>Evaluation of Management Comments.....</b>	<b>9</b>
<b>Scope and Methodology.....</b>	<b>10</b>
<b>Status of Prior Year Findings.....</b>	<b>13</b>
<b>Management Comments.....</b>	<b>15</b>
<b>Number of Controls Reviewed for Each System .....</b>	<b>17</b>
<b>Acronyms .....</b>	<b>20</b>



# Summary of Results

The Federal Information Security Modernization Act of 2014<sup>1</sup> (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems<sup>2</sup>, including those provided or managed by another agency, contractor, or other source. Because the Overseas Private Investment Corporation (OPIC or Corporation) is a federal agency, it is required to comply with federal information security requirements.

FISMA also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) 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 (NIST) are mandatory for Federal agencies.

The U.S. Agency for International Development (USAID) Office of Inspector General engaged us, Brown & Company CPAs and Management Consultants, PLLC, 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 selected security controls for certain 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 two OPIC-managed systems and four applications managed by external contractors.

---

<sup>1</sup> The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002.

<sup>2</sup> According to NIST, an information system is a discrete setoff information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

## Results

We concluded that OPIC generally complied with FISMA by implementing 65 of 72<sup>3</sup> security controls reviewed for selected information systems. For example, OPIC did the following:

- Implemented effective audit log monitoring, review and analysis.
- 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.
- Implemented multifactor authentication for remote access.

Although OPIC generally had policies for its information security program, its implementation of those policies for 7 of 72 security controls reviewed 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. Specifically, OPIC needs to:

- Update its Privacy Impact Assessments.
- Mitigate network vulnerabilities.
- Improve account management procedures.
- Review and update Interconnection Security Agreements.
- Strengthen enterprise architecture controls.

This report makes seven recommendations to assist OPIC in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to one prior year recommendation had not yet been fully addressed. Detailed findings appear in the following section.

---

<sup>3</sup> See Appendix IV for the controls tested.

# Audit Findings

## OPIC Needs to Update Its Privacy Impact Assessments

National Institute of Standards and Technology Special Publication (SP) 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, security control AR-2, Privacy Impact and Risk Assessment, states the following:

The organization:

\*\*\*

- b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Security control AR-1, Governance and Privacy Program, states the following:

\*\*\*

- f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].

In addition, *Overseas Private Investment Corporation Network System Security Plan (OPIC SSP)* dated June 2017, states that the network system contains Personal Identifiable Information (PII), and that a PIA is necessary. Also, the OPIC SSP lists applicable laws for its General Support System (GSS) to include compliance with the Privacy Act of 1974 as amended [5 United States Code 552a].

However, the *OPIC Privacy Impact Assessment* for its GSS dated August 9, 2012 and PIA for one external system dated March 27, 2015 were not updated to support the most recent OPIC SSP dated June 2017. This occurred because management did not prioritize resources to update the PIAs. As a result of this weakness, the PIAs may no longer reflect OPIC's current environment. Therefore, we are making the following recommendation.

**Recommendation 1:** We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement a process to update its Privacy Impact Assessments for the Corporation's information systems.

## OPIC Needs to Mitigate Network Vulnerabilities

NIST SP 800-53, Rev. 4, security control SI-2, Flaw Remediation, 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.

NIST SP 800-53, Rev. 4, security control RA-5, Vulnerability Scanning, states the following:

The organization:

\* \* \*

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

A vulnerability is a design flaw or incorrect configuration which makes the Agency's network (or host on the network) susceptible to malicious attacks from local or remote users. OPIC did not have an effective process in place to remediate vulnerabilities within patch cycles. For example, fiscal year (FY) 2018 independent scans performed using Qualys identified 575 vulnerabilities, including 65 "Urgent," 138 "Critical," 209 "Serious," 157 "Medium," and 6 "Minimal" level risk vulnerabilities related to weaknesses in patch and configuration management.

The reason OPIC has not resolved these vulnerabilities is because they relate to OPIC's servers and workstations with outdated Windows operating systems which the Corporation plans to upgrade or replace. OPIC is in the process of developing a strategy to address identified vulnerabilities by ensuring that new Windows 10 and Windows Server 2016 images are fully patched prior to being introduced in the environment and then replace existing workstations and servers with those machines.

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

- An attacker may leverage known issues to execute arbitrary code.
- The Corporation's employees may be unable to access systems.
- The Corporation's data may be compromised.

**Recommendation 2:** We recommend that the Overseas Private Investment Corporation Chief Information Officer remediate patch 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 3:** We recommend that the Overseas Private Investment Corporation Chief Information Officer document and implement a process to verify that patches are timely applied.

## OPIC Needs to Improve Account Management Procedures

NIST SP 800-53, Rev. 4, security control AC-2, Account Management, states the following regarding account management:

The organization:

\*\*\*

- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- g. Monitors the use of information system accounts;
- h. Notifies account managers:
  - 1. When accounts are no longer required;
  - 2. When users are terminated or transferred; and
  - 3. When individual information system usage or need-to-know changes.

In addition, security control AC-2, Control Enhancements, include the following:

- (1) Account Management | Automated System Account Management  
The organization employs automated mechanisms to support the management of information system accounts.
- (2) Account Management | Removal of Temporary / Emergency Accounts  
The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].
- (3) Account Management | Disable Inactive Accounts  
The information system automatically disables inactive accounts after [Assignment: organization-defined time period].
- (4) Account Management | Automated Audit Actions  
The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

The *OPIC Office of the Chief Information Officer (OCIO) /Information Security Access Control Procedure*, section “OPIC Information Owners,” states the following:

OPIC Information Owners are responsible for:

- a. Determining who should have access to their resources.
- b. Ensuring that their resources are protected against unauthorized access.
- c. Periodically reviewing access permissions.
- d. Assisting System Owners with controlling access to and protecting their resources, including wireless and/or mobile computing devices and remote access.
- e. Promptly removing access from a system when requested.
- f. Reporting any unauthorized access they discover.

The OPIC SSP, security control AC 2(3), “Disable Inactive Accounts,” requires the Corporation to disable inactive user accounts after 30 days. In addition, the OPIC SSP states that OPIC manages all information system accounts using its online account management system, which contains a checklist that is used for hiring, transfer, and termination actions for all OPIC staff. It also states that OPIC uses Microsoft Active Directory for account management, which allows for the management of account settings. It further states that when a user no longer needs access to systems or is leaving OPIC, the account management system is updated, and a notice enters the Help Desk queue to have the account disabled.

However, OPIC has not consistently implemented its account management procedures for all information system accounts. For example, we reviewed a system generated list of 413 OPIC active users from an account management system report as of June 27, 2018 and requested the Active Directory status for 18 of 413 active user accounts. We noted OPIC did not disable 3 of the 18 inactive user accounts after 30 days in accordance with Agency access control policy and procedures. Specifically, there were three inactive user accounts open for 82 days, 62 days, and 46 days, respectively. We also reviewed 10 of 128 separated user accounts from the “Separated Users” report and noted there was one separated user account open for 69 days after the separation date.

This occurred because OPIC did not allocate resources to implement effective procedures to notify account managers:

- When accounts are no longer required;
- When users are terminated or transferred; and/or
- When individual information system usage or need-to-know changes.

Therefore, OPIC’s managers could not effectively monitor the use of information system accounts and update the account management system on a regular basis. As a result of this weakness, OPIC has an increased risk of unauthorized access to its information and information systems.

OPIC also could not provide the dates the active accounts were disabled or deleted to confirm that user accounts were deactivated or deleted in a timely manner. This occurred because OPIC lacks procedures to ensure the account management system is updated for inactive accounts before the Help Desk disables the account. As a result of this weakness, OPIC cannot provide a complete audit trail of users’ account status. Therefore, we are making the following recommendations.

**Recommendation 4:** We recommend that the Overseas Private Investment Corporation Chief Information Officer document and implement a process to verify (1) the account management system is timely updated to support the management of information system accounts and (2) inactive accounts are timely disabled after 30 days in accordance with the Corporation’s access control procedures.

**Recommendation 5:** We recommend that the Overseas Private Investment Corporation Chief Information Officer document and implement procedures to record the date that system user accounts are disabled or deleted.

## OPIC Needs to Review and Update Interconnection Security Agreements

NIST SP 800-53, Rev. 4, security control CA-3, System Interconnections, states the following:

The organization:

\*\*\*

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

The OPIC SSP, security control CA-3, "System Interconnections", requires the Corporation to annually review and update Interconnection Security Agreements (ISAs).

OPIC has authorized a connection from its GSS to three information systems outside of the GSS accreditation boundary and executed the appropriate ISAs or Memorandum of Understandings (MOUs). However, OPIC does not have an effective process in place to ensure ISAs and MOUs are reviewed by management on an annual basis. For example, an ISA between a vendor, the General Service Administration and OPIC dated June 22, 2015 has not been reviewed and updated to include OPIC's current policies and procedures and names of Information Technology (IT) personnel, as required.

Also, the MOU and ISA signed on September 10, 2015, between OPIC and a shared service provider, was not reviewed annually, as required. Therefore, the MOU and ISA expired after three years ending September 10, 2018, without the Corporation's knowledge. This occurred because OPIC has not defined a process to update and monitor MOUs and ISAs. As a result of this weakness, OPIC cannot ensure it is in compliance with the MOUs and ISAs and that they are current and accurate. Therefore, we are making the following recommendation.

**Recommendation 6:** We recommend that the Overseas Private Investment Corporation Chief Information Officer document and implement a process to verify that Interconnection Security Agreements and Memorandum of Understandings are annually reviewed and, if needed, updated.

## OPIC Needs to Provide Contingency Training and Test the Contingency Plan

NIST Special Publication 800-53, Rev. 4, security control CP-3, Contingency Training, states the following:

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

- a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;
- b. When required by information system changes; and
- c. [*Assignment: organization-defined frequency*] thereafter.



In addition, security control CP-4, Contingency Plan (CP) Testing, states the following:

The organization:

- a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
- b. Reviews the contingency plan test results; and
- c. Initiates corrective actions, if needed.

The *OPIC OCIO/Security Contingency Planning Policy*, security control CP-3, “Contingency Training”, states the following:

- a. System Owners shall ensure that all personnel involved in information system contingency planning efforts are identified and trained in the procedures and logistics of information system contingency planning and implementation for systems under their purview and in compliance with NIST SP 800-34. Refresher training shall be provided annually.

In addition, security control CP-4, “Contingency Plan Testing and Exercises”, states the following:

- a. System Owners shall ensure that contingency plans for systems are tested/exercised at least annually in compliance with NIST SP 800-34.

OPIC did not provide contingency training or test its CP in FY 2018, as required. OPIC’s CP was last tested on June 7, 2017. OPIC officials said that this occurred because OPIC lacked the resources to provide the annual contingency training and had pulled out of a planned interagency Continuity of Operations Plan exercise in 2018 due to resource constraints, primarily consisting of limited manpower to support the event.

By not conducting contingency training or testing its contingency plan, in the event of an emergency, OPIC faces an increased risk that its plan may not be viable and that personnel, who must execute information system contingency plans, will not be trained in their responsibilities to ensure that any delay in recovering critical systems would be minimal. Therefore, we are making the following recommendation.

**Recommendation 7:** We recommend that the Overseas Private Investment Corporation’s Chief Information Officer conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC’s policy.

# Evaluation of Management Comments

In response to the draft report, the Overseas Private Investment Corporation (OPIC) provided comments and planned actions for all recommendations. OPIC agreed with recommendations 1 through 4, 6 and 7 and provided target dates for each recommendation. Therefore, we consider these recommendations resolved, but will remain open until OPIC provides IG with evidence that the planned corrective actions have been implemented.

OPIC disagreed with recommendation 5 because the Corporation has already configured automatic alerts in its centralized log aggregation tools to identify when an account [system's user account] is disabled or deleted. Based on OPIC's comments and our review of Active Directory and system log reports, we determined that OPIC's system user account disabling and deletion events are fully captured with date and time stamp. Therefore, recommendation 5 is resolved and closed. OPIC's comments are included in their entirety in Appendix III.

Based on our evaluation of management comments, we acknowledge management decisions on all seven 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 OPIC implemented selected security controls for certain information systems<sup>4</sup> in support of the Federal Information Security Modernization Act of 2014.

Our overall objective was to evaluate OPIC's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of OPIC's IT security program in accordance with U.S. Department of Homeland Security's (DHS) FISMA Inspector General reporting requirements:

- Risk Management;
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of OPIC's IT security governance structure and the Corporation's system security assessment and authorization (SA&A) methodology. We also followed-up on outstanding recommendations from prior FISMA audits (see Appendix II), and performed fieldwork on 2 of 2 OPIC-managed systems and on 4 of 4 external systems. The audit also included a vulnerability assessment of an OPIC-managed system and an evaluation of OPIC's process for identifying and mitigating technical vulnerabilities.

---

<sup>4</sup> See Appendix IV for a list of controls selected.

## Methodology

We reviewed OPIC's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also audited an internal system and OPIC's SA&A process. We considered the internal control structure for OPIC's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over OPIC's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of the systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to OPIC'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 FY 2015, 2016, and 2017 FISMA audit report; and
- Completed a network vulnerability assessment of OPIC's sole internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for OPIC's systems taken as a whole.

The criteria used in conducting this audit included:

- Public Law 113-283, Federal Information Security Modernization Act of 2014;
- FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- NIST SP 800-12, Revision 1, *An Introduction to Computer Security: The NIST Handbook*;
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard Publication 201-2, *Personal Identity Verification of Federal Employees and Contractors*; and
- Other criteria as appropriate.

The audit was conducted at OPIC's headquarters in Washington, D.C., from June 13, 2018 through October 4, 2018.

# Status of Prior Year Findings

No.	FY 2017 <sup>5</sup> , 2016 <sup>6</sup> and 2015 <sup>7</sup> Audit Recommendations	Status	Auditor's Position on Status
1	<b>FY 2017 FISMA audit recommendation No. 1:</b> <i>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.</i>	Open	Agree
2	<b>FY 2017 FISMA audit recommendation No. 2</b> <i>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.</i>	Closed	Agree
3	<b>FY 2017 FISMA audit recommendation No. 3:</b> <i>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</i>	Closed	Agree
4	<b>FY 2016 FISMA audit recommendation No. 5:</b> <i>We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement multifactor authentication for network user accounts and document the results as required by the Cybersecurity Strategy and Implementation Plan.</i>	Closed	Agree

<sup>5</sup> The Overseas Private Investment Corporation Implemented Controls In Support of FISMA For Fiscal Year 2017, But Improvements Are Needed (Audit Report No. A-OPC-17-007-C, September 28, 2017).

<sup>6</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).

<sup>7</sup> 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-15-009-P), September 17, 2015.

## APPENDIX II

No.	FY 2017 <sup>5</sup> , 2016 <sup>6</sup> and 2015 <sup>7</sup> Audit Recommendations	Status	Auditor's Position on Status
5	<p><b>FY 2016 FISMA audit recommendation No. 7:</b> <i>We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement asset management procedures to include processes for ensuring information system assets are inventoried on an organization-defined frequency.</i></p>	Closed	Agree
6	<p><b>FY 2016 FISMA audit recommendation No. 10:</b> <i>We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement an enterprise architecture methodology in line with Federal Enterprise Architecture and Risk Management Framework.</i></p> <p>OPIC accepted the risk of not implementing an enterprise architecture methodology and closed this recommendation.</p>	Closed	Agree
7	<p><b>FY 2015 FISMA audit recommendation No 1:</b> <i>We recommend that the Overseas Private Investment Corporation Chief Information Officer implement a documented process to periodically review service accounts to determine whether accounts are necessary and disable accounts no longer required.</i></p>	Closed	Agree

# Management Comments



MEMORANDUM

November 20, 2018

**TO:** Alvin Brown, Deputy Assistant Inspector General, United States Agency for International Development Office of the Inspector General

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

**SUBJECT:** **Overseas Private Investment Corporation Response to the Audit of the Overseas Private Investment Corporation’s Fiscal Year 2018 Compliance with Provisions of the Federal Information Security Modernization Act of 2014**

Below is the Overseas Private Investment Corporation’s (OPIC) response to the Office of Inspector General’s (OIG) DRAFT report “OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (A-OPC-19-00X-C).”

The Inspector General report contains seven (7) 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 90% (65/72) of the security controls tested.

**Recommendation 1:** Document and implement a process to update its Privacy Impact Assessments for the Corporation’s information systems.

**Management Response:** OPIC will develop and implement a process to ensure that OPIC’s PIAs are revalidated at the frequency established in OPIC’s Privacy Policy. Target due date: May 31, 2019.

**Recommendation 2:** Remediate patch and configuration 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.

**Management Response:** OPIC acknowledges the risk of patch and configuration vulnerabilities and will continue with its ongoing effort to address these weaknesses by completing its current OS modernization project. OPIC will upgrade all Windows 7 workstations to fully-patched and CIS benchmark-compliant

Overseas Private Investment Corporation  
1100 New York Avenue, NW  
Washington, D.C. 20527  
202.336.8400 | [www.opic.gov](http://www.opic.gov)



Windows 10 workstations. Similarly, OPIC will upgrade its Windows 2008 Servers to fully-patched and CIS benchmark-compliant Windows 2016 servers. Target due date: February 28, 2019.

**Recommendation 3:** Document and implement a process to verify that patches are applied in a timely manner.

**Management Response:** OPIC will develop and implement a patch strategy and process to ensure that all network assets are patched within 30 days from the date a patch becomes available in compliance with the risk tolerance defined by the Agency. Target due date: February 28, 2019.

**Recommendation 4:** Document and implement a process to verify (1) the account management system is updated promptly to support the management of information system accounts and (2) inactive accounts are promptly disabled after 30 days in accordance with the Corporation's access control procedures.

**Management Response:** OPIC will review its process to disable inactive accounts and identify improvements or automation to mitigate the risk of inactive accounts older than 30 days. Target due date: March 30, 2019.

**Recommendation 5:** Document and implement procedures to record the date that system user accounts are disabled or deleted.

**Management Response:** OPIC acknowledges that recording these events is important but disagrees that this is a deficiency. OPIC already records these events in AD automatically. In addition, OPIC has already configured automatic alerts in its centralized log aggregation tool (Splunk) to identify when an account is disabled and deleted. No further action is necessary.

**Recommendation 6:** Document and implement a process to verify that interconnection security agreements and memorandums of understanding are annually reviewed, and if needed, updated.

**Management Response:** OPIC will review its current interconnection security agreement procedure to identify areas of improvement. Upon review, OPIC will document and implement necessary corrective actions to ensure that agreements are kept current. Target due date: April 30, 2019.

**Recommendation 7:** Conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC's policy.

**Management Response:** OPIC will train personnel with relevant CP responsibilities on the updated version. OPIC will also schedule and perform contingency plan tests as required by policy. Target due date: July 30, 2019.

My primary point of contact for this matter is Mr. James Wolff, Acting Chief Information Officer, 202-336-8673, [james.wolff@opic.gov](mailto:james.wolff@opic.gov).

/s/

**Michele Perez**  
**VP, Department of**  
**Management and**  
**Administration**

Overseas Private Investment Corporation  
1100 New York Avenue, NW  
Washington, D.C. 20527  
202.336.8400 | [www.opic.gov](http://www.opic.gov)

# Number of Controls Reviewed for Each System

Control No.	Control Name	Number of Systems Tested
AC-1	Access Control Policy & Procedures	1
AC-2	Account Management	1
AC-5	Separation of Duties	3
AC-8	System Use Notification	1
AC-17	Remote Access	1
AC-20	Use of External Information Systems	6
AR-2	Privacy Impact And Risk Assessment,	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
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
CM-1	Configuration Management Policy & Procedures	1
CM-2	Baseline Configuration	1
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	1
CM-9	Configuration Management Plan	1
CM-10	Software Usage Restrictions	1
CP-1	Contingency Planning Policy & Procedures	1

## APPENDIX IV

Control No.	Control Name	Number of Systems Tested
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
IA-1	Identification & Authentication Policy and Procedures	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
PL-2	System Security Plan	1
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-9	Risk Management Strategy	1
PM-11	Mission/Business Process Definition	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	1
RA-5	Vulnerability Scanning	1
SA-3	System Development Life Cycle	1
SA-4	Acquisitions Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	2
SI-2	Flaw remediation	1

## APPENDIX IV

Control No.	Control Name	Number of Systems Tested
SI-4	Information System Monitoring	1
SE-1	Inventory of Personally Identifiable Information	1
SE-2	Privacy Incident Response	1
DM-1	Minimization of Personally Identifiable Information	1
DM-3	Minimization of PII Used in Testing, Training, and Research	1
AR-5	Privacy Awareness and Training	1
SC-28	Protection of Information at Rest	1
SC-7	Boundary Protection	1
	<b>Total Controls</b>	<b>72</b>

# Acronyms

Acronyms	
IG	Inspector General
DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GSS	General Support System
ISA	Interconnection Security Agreement
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	U.S. Office of Management and Budget
OPIC	Overseas Private Investment Corporation
PIA	Privacy Impact Assessments
PII	Personal Identifiable Information
Rev.	Revision
SA&A	Security Assessment and Authorization
SP	Special Publication
SSP	System Security Plan