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

OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019

AUDIT REPORT A-OPC-20-003-C
JANUARY 16, 2020

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, Millennium Challenge Corporation, U.S. African Development Foundation, Inter-American Foundation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: 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 16, 2020

TO: U.S. International Development Finance Corporation, Chief Executive Officer, Adam Boehler

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

SUBJECT: OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019 (A-OPC-20-003-C)

Enclosed is the final audit report on the Overseas Private Investment Corporation's (OPIC's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2019. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the audit. [1] The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA'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. CLA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which CLA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether OPIC implemented an effective information security program.[2] To answer the audit objective, CLA tested OPIC's implementation of selected management, technical, and operational 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." CLA auditors reviewed all three

[1] Under the Better Utilization of Investments Leading to Development (BUILD) Act of 2018, OPIC and components of USAID merged to create the U.S. International Development Finance Corporation (DFC). USAID OIG will provide oversight until an Inspector General for DFC is appointed.

[2] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

information systems in OPIC's systems inventory as of June 2019. Fieldwork took place at OPIC's headquarters in Washington, DC, from June 6 to October 4, 2019. The audit covered the period from October 1, 2018, through September 30, 2019.

CLA concluded that OPIC generally implemented an effective information security program by implementing 58 of 71 selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of its information and information systems. Among the controls OPIC implemented were the following:

- An assessment and authorization process, including controls around planning, risk assessments, and security assessment and authorization
- An information system continuous monitoring program
- Security training processes and program
- An incident handling and response program
- A configuration and change management program

However, in five of the eight FISMA metric domains, CLA noted weaknesses that may expose OPIC's information and information systems to unauthorized access, use, disclosure, disruption, modification, or destruction (see table below).

Fiscal Year 2019 IG FISMA Metric Domains[3]	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	X

The weaknesses occurred because OPIC did not complete the following: timely remediate system vulnerabilities, update privacy impact assessments for three systems, disable inactive accounts, conduct contingency testing and training, maintain current agreements for backup telecommunications, maintain an up-to-date inventory of information system components, fully document its enterprise architecture strategy, and provide proper oversight of information technology contractors.

[3] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 9, 2019.

The weaknesses related to system vulnerabilities, privacy impact assessments, inactive accounts, and contingency testing and training were raised in previous years. Since recommendations to address these issues were made previously and have not been closed, we are not repeating them in this report. To address the other weaknesses identified in the report, we recommend that OPIC's chief information officer:

Recommendation 1: Document and implement a process to maintain current and up-to-date agreements for backup telecommunications.

Recommendation 2: Implement asset management procedures to include processes for ensuring information system assets are inventoried on an organization-defined frequency.

Recommendation 3: Complete the enterprise architecture strategy to be in line with the Federal enterprise architecture and risk management framework.

Recommendation 4: Document and implement a process to verify oversight of information technology-related contractor roles and responsibilities.

In finalizing the report, CLA evaluated OPIC's responses to recommendations 1, 2, 3 and 4. After reviewing that evaluation, we consider recommendations 1, 2 and 3 resolved but open pending completion of planned activities, and recommendation 4 resolved but open pending OIG's verification of OPIC's final action. For recommendations 1 to 3, please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance extended to our staff and CLA's employees during the engagement.

Overseas Private Investment Corporation's
Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2019

Final Report

A member of Nexia International

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

December 17, 2019

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:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit of the Overseas Private Investment Corporation's (OPIC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2019.

We appreciate the assistance we received from the staff of OPIC and appreciate the opportunity to serve you. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Overseas Private Investment Corporation's (OPIC) information security program and practices for fiscal year 2019 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether OPIC implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls for all three information systems in OPIC's systems inventory. Audit fieldwork was performed at OPIC's headquarters in Washington, D.C., from June 6, 2019 to October 4, 2019.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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.

We concluded that OPIC generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. Although OPIC generally implemented an effective information security program, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in 5 of the 8 Inspector General FISMA Metric Domains and have made four recommendations to assist OPIC in strengthening its information security program.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on October 4, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 4, 2019.

The purpose of this audit report is to report on our assessment of OPIC's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to USAID Office of Inspector General.

CliftonLarsonAllen LLP

Arlington, Virginia
December 17, 2019

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual evaluation of the Overseas Private Investment Corporation's (OPIC or Corporation) information security program and practices. The objective of this performance audit was to determine whether OPIC implemented an effective[2] information security program.

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal Agency information security programs. FISMA 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.

FISMA also requires Agency Inspectors General (IGs) to assess the effectiveness of Agency information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish Agency baseline security requirements.

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA Reporting Metrics[3] to independently assess their agencies' information security programs.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of OMB with respect to Agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

[3] CLA submitted its responses to the FY 2019 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2019 IG FISMA Reporting Metrics are designed to assess the maturity[4] of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Reporting Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For this audit, CLA reviewed selected[5] controls related to the IG FISMA Reporting Metrics from all three information systems[6] in OPIC's FISMA inventory as of June 2019.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

Audit Results

We concluded that OPIC generally implemented an effective information security program by implementing 58 of 71[7] selected security controls for the 3 selected information systems. For example, OPIC:

- Maintained an effective assessment and authorization process, including controls around planning, risk assessments, and security assessment and authorization.

[4] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 – Optimized. To be considered effective, an agency's information security program must be rated *Managed and Measurable* (Level 4).

[5] See Appendix III for a list of controls selected.

[6] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[7] There were 67 NIST SP 800-53, Revision 4, controls specifically identified in the FY 2019 IG metrics. We tested the 65 controls that were applicable to systems within the scope of our audit. We also tested 2 additional privacy controls from Appendix J of NIST SP 800-53 Revision 4 because they related to the metrics. A control was counted for each system it was tested against. Thus, there were 71 instances of testing a control.

- Maintained an effective information system continuous monitoring program.
- Maintained and enhanced its security training processes and program.
- Maintained an effective incident handling and response program.
- Maintained an effective configuration and change management program.

Although OPIC generally implemented an effective information security program, its implementation of 13 of the 71 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. As a result, CLA noted weaknesses in the following FISMA Metric Domains (Table 2) and made four recommendations to assist OPIC in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2019 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Identify	**Risk Management**	OPIC Needs to Strengthen Enterprise Architecture Strategy (**Finding 6**) OPIC Needs to Strengthen Contractor Oversight (**Finding 7**)
Protect	**Configuration Management**	OPIC Needs to Strengthen Vulnerability and Patch Management Controls (**Finding 1**) OPIC Needs to Strengthen Asset Management Controls (**Finding 5**)
	Identity and Access Management	OPIC Needs to Strengthen Account Management Controls (**Finding 3**)
	Data Protection and Privacy	OPIC Needs to Ensure Privacy Program Documentation is Up-to-Date (**Finding 2**)
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	OPIC Needs to Strengthen Contingency Planning Controls (**Finding 4**)

In response to the draft audit report, OPIC outlined and described its plans to address recommendations 1, 2 and 3 and disagreed with recommendation 4. Based on our

evaluation of management's comments, we acknowledge OPIC's management decisions on recommendations 1, 2 and 3. Further, we consider recommendations 1, 2 and 3 resolved, but open pending completion of planned activities. In addition, we consider recommendation 4 resolved, but open pending OIG's verification of the Agency's final actions. OPIC's comments are included in their entirety in Appendix II.

The following section provides a detailed discussion of the audit findings. Appendix I describes the audit scope and methodology.

AUDIT FINDINGS

1. OPIC Needs to Strengthen Vulnerability and Patch Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Configuration Management*

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security control SI-2, states the following regarding patch management:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [*Assignment: organization defined time period*] of the release of the updates.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states:

> i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.
>
> Agencies shall:
> * * *
> 8. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement.
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

CLA performed independent scans using the software tool Nessus noted vulnerabilities on one of OPIC's systems based on Common Vulnerabilities and Exposures[8] identification. CLA noted critical and high vulnerabilities from 2018 and earlier related to missing patches, configuration weaknesses, and unsupported software. Specifically, hosts were missing patches that were released for Oracle WebLogic, Microsoft NET Framework, Microsoft Office products, Oracle Java and Adobe Flash Player. In addition, Registry[9] configuration weaknesses prevented the effectiveness of multiple Microsoft patches. The unsupported software was related to Adobe Acrobat, Apple QuickTime, Microsoft Visio, RSA SecurID Software Token, WinZip and Oracle WebLogic.

[8] Common Vulnerabilities and Exposures is a dictionary of common names for publicly known IT system vulnerabilities. (Source: NIST Special Publication 800-51, Revision 1, *Guide to Using Vulnerability Naming Schemes*).

[9] Registry is a database containing data critical for operation of Microsoft operating systems, applications and services.

During FY 2019, OPIC began a process to identify vulnerabilities that were outside of specified remediation timeframes; however, we noted that the timely remediation of vulnerabilities remains delayed. OPIC was aware of most of the identified vulnerabilities and has documented a plan to remediate vulnerabilities in a defined timeframe; however, older vulnerabilities and configuration weaknesses remain. OPIC planned to remediate the older issues through the Plan of Action and Milestone (POA&M) process by December 2019.

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 that will fix the 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 on OPIC's network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Authorized OPIC employees may be unable to access systems.
- OPIC data may be lost, stolen, or compromised.

Furthermore, unsupported systems may be susceptible to older vulnerabilities and exploits that vendors have addressed with current supported versions.

Recommendations addressing this finding were issued in the FY 2018 FISMA audit.[10] OPIC plans to take final corrective action during FY 2020. Therefore, we are not making a new recommendation at this time.

2. OPIC Needs to Ensure Privacy Program Documentation is Up-to-Date

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, privacy control AR-2, states the following regarding privacy impact and risk assessment:

> 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.

OPIC's *Privacy Policy*, Section 7.2 Privacy Impact Assessments, states "(2) As determined by the PTA,[11] conduct PIAs of the systems every three years or when a

[10] Recommendation 2 and 3, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).
[11] A PTA is completed to determine what Personally Identifiable Information is contained in the system.

change occurs as defined by *NIST SP 800-53a, Guide for Assessing the Security Controls in Federal Information System*, that creates a new privacy risk." In addition, System Owners must, "(4) review and revalidate the contents of their systems' PIA(s) biennially, or upon significant changes as needed, and document the results of each PIA review."

OPIC has not conducted PIAs in over three years as required by its *Privacy Policy*. The PIAs for three systems were dated between FY 2012 and FY 2015. OPIC had implemented a notification process for PIAs that were out of date; however, OPIC had elected to suspend updates to the PIA's pending the establishment of the new agency.[12]

Without properly assessing the privacy impact of each information system, OPIC may be unaware of what current privacy risk each system poses to the environment.

A recommendation addressing this finding was issued in the FY 2018 FISMA audit.[13] Since that recommendation is still open, we are not making a new recommendation at this time.

3. OPIC Needs to Strengthen Account Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Identify and Access Management*

NIST SP 800-53, Revision 4, security control AC-2, 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].
> * * *
> 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.

Controls were not adequate to ensure OPIC performed effective account management controls for the three sampled systems tested. Specifically, we noted the following account management control weaknesses for inactive and terminated users:

- For one sampled system, from the total population of 487 user accounts, 8 accounts were not disabled after 30 days of inactivity in accordance with OPIC's policy for the system.
- For a second sampled system, from the total population of 334 user accounts, 1 account was not disabled after 90 days of inactivity in accordance with OPIC's policy for the system.

[12] The *Better Utilization of Investments Leading to Development (BUILD) Act*, signed on October 5, 2018, resulted in the combination of OPIC and USAID's *Development Credit Authority* into the U.S. International Development Finance Corporation (DFC) at the beginning of Fiscal Year 2020.

[13] Recommendation 1, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).

- For a third sampled system, from the total population of 108 user accounts, 9 accounts were not disabled after 90 days of inactivity in accordance with OPIC's policy for the system. Additionally, 3 accounts belonged to separated users that retained active accounts after termination.

In addition, 8 out of 9 sampled user accounts from the first system did not have evidence of timely account disabling. Specifically, OPIC tracks employee separations through its human resource tool; however, these accounts were not consistently disabled timely or recorded in the human resource tool as having cleared the Helpdesk for account disabling. Further, OPIC did not have an alternative method of showing that accounts were disabled timely for separated personnel.

Also, for the first system OPIC was not reviewing accounts that had never been logged onto and the automated controls in place did not detect these accounts. Additionally, for separated individuals and associated accounts, OPIC had an open POA&M; however, due to the planned agency change at the end of the fiscal year, corrective action was not prioritized.

Without effective access controls, OPIC information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. Inactive accounts that are not disabled in accordance with Agency policy and user accounts that are not disabled when employees separate may be used to gain access to the Agency's data and sensitive information. In addition, the lack of comprehensive periodic account reviews can lead to system users with greater access than is required to perform their job functions and/or segregation of duties issues.

A recommendation addressing this finding was issued in the fiscal year 2018 FISMA audit.[14] OPIC plans to take final corrective action during fiscal year 2020. Therefore, we are not making a new recommendation at this time.

4. OPIC Needs to Strengthen Contingency Planning Controls

Cybersecurity Framework Security Function: *Recover*
FY 19 FISMA IG Metric Domain: *Contingency Planning*

NIST SP 800-53, Revision 4, security control CP-3, states the following regarding contingency training, "The Organization provides contingency training to information system users consistent with assigned roles and responsibilities".

OPIC's *NIST 800-53 Security Controls OPIC Organizational Parameters*, CP-3, states the following:

> The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
> a. Within annually of assuming a contingency role or responsibility;
> b. When required by information system changes; and
> c. Annually thereafter.

[14] Recommendation 4, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).

NIST SP 800-53, Revision 4, security control CP-4, states the following regarding contingency plan testing:

> The organization:
> a. Tests the contingency plan for the information system [*organization-defined frequency*] using [*organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan.

Additionally for CP-4, "The organization tests the contingency plan for the information system at least annually for high and moderate impact systems using function exercise for high and moderate impact systems to determine the effectiveness of the plan and the organizational readiness to execute the plan."

NIST SP 800-53, Revision 4, security control CP-8, states the following regarding telecommunications services:

> The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*organization-defined time period*] for essential missions and business functions within [*organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing and storage sites.

OPIC has not conducted contingency testing and training for FY 2019. Due to competing priorities, contingency plan testing and training was delayed. In addition, OPIC had not maintained a current agreement for backup telecommunications. The agreement had expired in September 2018. This occurred because OPIC did not have a process in place to maintain the agreements.

OPIC had an open POA&M in place for the contingency plan testing and training; however, due to the planned change in the agency at the end of the fiscal year, OPIC had not prioritized completion and moved the POA&M closure into FY 2020. In addition, OPIC management had not maintained copies of agreements with external service providers.

Without completing training and testing of the contingency plan, OPIC may be unprepared for a real world event. Additionally, without having proper agreements in place, OPIC is at risk of not having services available when they are needed.

A recommendation addressing the lack of contingency testing and training weaknesses was issued in the fiscal year 2018 audit.[15] OPIC had not yet taken corrective action and therefore, we are not making a new recommendation at this time. However, we are making a recommendation to address the weakness with OPIC's backup telecommunications agreement.

> ***Recommendation 1:*** *The Overseas Private Investment Corporation's Chief Information Officer should document and implement a process to maintain current and up-to-date agreements for backup telecommunications.*

[15] Recommendation 7, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).

5. OPIC Needs to Strengthen Asset Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Configuration Management*

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's *NIST 800-53 Security Controls OPIC Organizational Parameters*, CM-8, states, "Reviews and updates the information system component inventory quarterly."

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. 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.

> ***Recommendation 2:*** *We recommend the OPIC Chief Information Officer implement asset management procedures to include processes for ensuring information system assets are inventoried on an organization-defined frequency.*

6. OPIC Needs to Strengthen Enterprise Architecture Strategy

Cybersecurity Framework Security Function: *Identify*
FY 19 FISMA IG Metric Domain: *Risk Management*

NIST Special Publication 800-53, Revision 4, security control PM-7, states the following regarding Enterprise Architecture (EA):

> 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 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 with the enterprise and security architecture.

OMB Circular A-130, *Managing Information as a Strategic Resource*, states the following regarding Enterprise Architecture:

> Agencies shall develop an EA that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. The EA should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state to the desired future state, helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

OPIC's Office of the Chief Information Officer (OCIO) developed a roadmap that describes the IT challenges and goals for the corporation. However, the roadmap does not fully incorporate all requirements of an enterprise architecture strategy to include resulting risk to individuals, other organizations and the Nation. In addition, the roadmap did not correlate the represented plans to agency strategic plans supporting mission and business functions.

OPIC's enterprise architecture strategy was not fully documented due to the planned transition to the U.S. International Development Finance Corporation. In addition, OPIC management indicated their resources were limited to adequately plan for enterprise architecture during the transition.

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.

> ***Recommendation 3:*** *We recommend the OPIC Chief Information Officer complete the enterprise architecture strategy to be in line with the Federal enterprise architecture and risk management framework.*

7. OPIC Needs to Strengthen Contractor Oversight

Cybersecurity Framework Security Function: *Identify*
FY 19 FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control SA-5, states the following regarding an organizational privacy plan, policies, and procedures:

> The organization:
> * * *
> d. Protects documentation as required, in accordance with the risk management strategy; and
> e. Distributes documentation to [organization-defined personnel or roles].

OPIC's *NIST 800-53 Security Controls OPIC Organizational Parameters*, SA-5, states, "Distributes documentation to System Owner, Information System Security Officer (ISSO), and applicable Technical Support Staff."

OPIC was unable to provide documentation to support the following: individuals with remote access to one sampled system, system backups, and an inventory of media sanitized during FY 2019. This information was requested from OPIC's operations team; however, due to a transition in contractors, the information was not available.

OPIC had a transition in contractor staffing which occurred during the year for Infrastructure Operations. However, OPIC did not provide proper oversight during the transition of contractors to ensure all roles and responsibilities were conducted and properly transitioned to the new contractors.

Without the proper oversight of the contractors and support teams at OPIC, there is the possibility that proper agreed upon procedures may not be conducted by the contractors.

> ***Recommendation 4:*** *We recommend the OPIC Chief Information Officer document and implement a process to verify oversight of information technology-related contractor roles and responsibilities.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, OPIC outlined its plans to address recommendations 1, 2, and 3 and disagreed with recommendation 4. OPIC's comments are included in their entirety in Appendix II.

Based on our evaluation of management's comments, we acknowledge OPIC's management decisions on recommendations 1, 2 and 3. Further, we consider recommendations 1, 2 and 3 resolved, but open pending completion of planned activities.

In regard to recommendation 4, we reviewed OPIC's management's comments, which indicated that the contractor transition was the cause as well as the solution for issues identified. CLA understands OPIC's rationale; however, at the time of the audit, the process was not apparent and information was not available to support the audit. Therefore, there has not been sufficient time to determine if OPIC's corrective actions and implemented process corrected the weaknesses identified. We consider recommendation 4 resolved, but open pending OIG's verification of the Agency's final actions.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with GAGAS. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit was designed to determine whether OPIC implemented an effective[16] information security program.

The audit included tests of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed OPIC's performance and compliance with FISMA in the following areas:

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

For this audit, CLA reviewed selected controls related to the FY 2019 IG FISMA Reporting Metrics from all 3 information systems in OPIC's systems inventory as of June 2019. See Appendix III for a listing of selected controls.

The audit also included a follow up on prior audit recommendations (2017,[17] and 2018[18]) to determine if OPIC made progress in implementing the recommended improvements concerning its information security program. See Appendix IV for the status of prior year recommendations.

[16] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[17] *OPIC 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).

[18] *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (Audit Report No. A-OPC-19-006-C, January 30, 2019).*

Audit fieldwork was performed at OPIC's headquarters in Washington, D.C. from June 6, 2019 to October 4, 2019. It covered the period from October 1, 2018, through September 30, 2019.

Methodology

To determine if OPIC implemented an effective information security program, CLA conducted interviews with OPIC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, CLA 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) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, CLA compared documents, such as OPIC's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. Further, CLA reviewed the status of open FISMA audit recommendations from fiscal year 2017 and 2018.[19]

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, 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 was considered. In some cases, this resulted in selecting the entire population. However, in cases where entire audit population was not selected, the results cannot be projected and if projected may be misleading.

To perform our audit of OPIC's information security program and practices, we followed a work plan based on the following guidance:

- OMB and DHS, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular Number A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations.*

[19] Ibid 16 and 17.

MANAGEMENT COMMENTS

MEMORANDUM December 6, 2019

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

FROM: Mark Rein
Chief Information Officer, Office of the Chief Information Officer (OCIO) - Overseas Private Investment Corporation (OPIC)

SUBJECT: OPIC Comments on the Audit of the Overseas Private Investment Corporation's Fiscal Year 2019 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 Generally Implemented Controls in Support of FISMA for Fiscal Year 2019 (A-OPC-20-00X-C).*"

The Inspector General report contains four (4) new 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 revision 2 are the foundation of OPIC's information system security program. As indicated in the report, OPIC's program successfully implemented 82% (58/71) of the security controls tested.

Recommendation No. 1: Document and implement a process to maintain current and up-to-date agreements for backup telecommunications.

Management Response: The OCIO agrees that this is an oversight and has taken steps toward resolution. All telecommunication agreements for external services will be placed in an accessible location and reviewed periodically. The appropriate OPIC policies will be updated to reflect the location and review periodicity. This response has been entered as line item OIG-2019-1 in the OPIC Plan of Action and Milestones (POA&M). OPIC's Risk Rating: **Low**. Target due date: **May 29, 2020.**

Recommendation No. 2: Implement asset management procedures to include processes for ensuring information system assets are inventoried on an organization-defined frequency.

Management Response: The OCIO agrees that this is a concern and has taken steps toward resolution. OPIC will rely on multiple automated tools (i.e. BigFix, Tenable Nessus, SolarWinds and Active Directory) to monitor the network environment and report changes in hardware. Periodic physical inventories will be conducted and compared with the automated reports to ensure consistency. The appropriate OPIC policies will be updated to reflect the target percentage of assets inventoried and review frequency. This response has been entered as line item OIG-2019-2 in the OPIC POA&M. OPIC's Risk Rating: **Moderate**. Target due date: **March 31, 2020**.

Recommendation No. 3: Complete the enterprise architecture strategy to be in line with the Federal Enterprise Architecture and Risk Management Framework.

Management Response: The OCIO agrees that this is an area of improvement and has taken steps toward resolution. OCIO will develop and document an agency-wide Enterprise Architecture strategy aligned with the Common Approach to Federal Enterprise Architecture, to include resulting risk to individuals, other organizations and the Nation. Furthermore, the strategy will correlate the represented plans to agency strategic plans supporting mission and business functions. This strategy will follow the guidance provided by NIST Special Publication (SP) 800-37 revision 2, NIST SP 800-53 rev 4 and NIST SP 800-39. OCIO will update the appropriate policies to reflect the latest Enterprise Architecture with consideration for information security and risk to the organization. This response has been entered as line item OIG-2019-3 in the OPIC POA&M. OPIC's Risk Rating: **Low**. Target due date: **April 30, 2020.**

Recommendation No. 4: Document and implement a process to verify oversight of information technology-related contractor roles and responsibilities.

Management Response: The OCIO disagrees with this finding as presented in this memo. During the audit period, OPIC was transitioning between contractors tasked with providing Information Technology Technical Services. The Statement of Work (SOW) for this effort clearly defined the roles and responsibilities of the selected vendor and OPIC to include Service Level Agreements, Standard Operating Procedures, Transition Plans and Performance Based Objectives. The selected vendor accepted the SOW which resulted in the contract award. The challenges came when the selected vendor failed to meet the objectives documented in the SOW which resulted in the circumstances surrounding this finding. By following the established "process to verify oversight of information technology-related contractor roles and responsibilities", OPIC was able to document the inability of the vendor to meet the standards set in the contract allowing the contract to be terminated.

/s/ Mark Rein

SUMMARY OF CONTROLS REVIEWED

The following table identifies the controls selected for testing.

Control	Control Name	Number of Systems Tested
AC-1	Access Control Policy and Procedures	1
AC-2	Account Management	3
AC-8	System Use Notification	1
AC-17	Remote Access	1
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	1
AR-4	Privacy Monitoring and Auditing	1
AR-5	Privacy Awareness and Training	1
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	1
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policy and 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 and Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing	1
CP-6	Alternate Storage Site	1
CP-7	Alternate Processing Site	1
CP-8	Telecommunications Services	1
CP-9	Information System Backup	1
IA-1	Identification and Authentication Policy and Procedures	1
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1

Control	Control Name	Number of Systems Tested
IR-7	Incident Response Assistance	1
MP-3	Media Marking	1
MP-6	Media Sanitization	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-8	Critical Infrastructure Plan	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
SA-3	System Development Life Cycle	1
SA-4	Acquisition Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	3
SA-12	Supply Chain Protection	1
SC-8	Transmission Confidentiality and Integrity	1
SC-28	Protection of Information at Rest	1
SE-2	Privacy Incident Response	1
SI-2	Flaw Remediation	1
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-7	Software, Firmware, and Information Integrity	1

STATUS OF PRIOR YEAR FINDINGS

The following tables provide the status of the FY 2017[20] and FY 2018[21] FISMA audit recommendations.

No.	FY 2017 Audit Recommendation	OPIC Position on Status	Auditor's Position on Status
1	Remediate network vulnerabilities identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.	Open	Agree

No.	FY 2018 Audit Recommendation	OPIC Position on Status	Auditor's Position on Status
1	Document and implement a process to update its privacy impact assessments for the Corporation's information systems.	Closed	Disagree, Refer to Finding 2
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.	Open	Agree
3	Document and implement a process to verify that patches are applied in a timely manner.	Closed	Disagree, Refer to Finding 1
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.	Open	Agree
5	Document and implement procedures to record the date that system user accounts are disabled or deleted.	Closed	Agree
6	Document and implement a process to verify that interconnection security agreements and memorandums of understanding are annually reviewed and, if needed, updated.	Closed	Agree
7	Conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC's policy.	Open	Agree

[20] *OPIC 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).

[21] *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (Audit Report No. A-OPC-19-006-C, January 30, 2019).*