OFFICE OF INSPECTOR GENERAL

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

WASHINGTON, DC

Please note that certain information contained in this transmittal memo and attached report has been redacted as "SBU" (sensitive but unclassified) by OPIC officials, meaning that public disclosure of this material could compromise the integrity of government computer systems and networks. All redactions are made under Freedom of Information Act Exemption 7(E).

Office of Inspector General

November 7, 2016

The Honorable Michele Perez
Vice President, Department of Management and Administration
Overseas Private Investment Corporation
1100 New York Avenue NW
Washington, DC 20527

Dear Ms.Perez:

Enclosed is the final report, "The Overseas Private Investment Corporation Has Implemented Many Controls In Support Of FISMA For Fiscal Year 2016, But Improvements Are Needed" (Report No. A-OPC-17-005-C). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. According to Clifton officials, they performed this audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Clifton's report and related audit documentation. Our review was different from an audit in accordance with U.S. generally accepted government auditing standards and was not intended to enable us to express, and we do not express, an opinion on the Overseas Private Investment Corporation's (OPIC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We did not find any instances in which Clifton did not comply, in all material respects, with applicable standards.

~~(SBU)~~ The audit objective was to determine whether OPIC implemented minimum security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested OPIC's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." The audit reviewed all of OPIC's systems: [redacted] Clifton conducted fieldwork at OPIC's headquarters in Washington, DC, from March 11 to June 29, 2016.

The audit concluded that OPIC implemented 84 of 105 security controls for selected information systems in support of FISMA. However, OPIC did not implement 21 controls designed to preserve the confidentiality, integrity, and availability of its information and information systems.

OPIC complied with many of the FISMA requirements, including the following:

- Implementing effective audit-log monitoring, review, and analysis.
- Categorizing its information systems and the information processed, stored, or transmitted in accordance with Federal guidelines, and designating senior officials to review and approve the security categorizations.
- Implementing system and service acquisition controls.
- Implementing change-management policy and procedures.

~~(SBU)~~ However, OPIC still needs to do the following, listed from the most to the least significant:

- Strengthen [redacted] over patch and configuration management.
- Periodically review network accounts, and strengthen account management controls.
- Strengthen [redacted] account management.
- [redacted]
- Strengthen authorization processes and security control assessments for [redacted]
- Strengthen [redacted] controls.
- Strengthen OPIC's asset management controls.
- Strengthen [redacted] separation of duties controls.
- Strengthen physical and environmental controls.
- Strengthen enterprise architecture controls.
- Update the incident response plan.
- Maintain training and rules of behavior records.
- Test the [redacted] contingency plan.
- Strengthen compliance of baseline configurations.
- Strengthen process for executing the plan of action and milestones.
- Assess [redacted] components.

To address the weaknesses identified in Clifton's report, OIG makes the following recommendations to OPIC's management.

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

~~(SBU)~~ ***Recommendation 2.*** *We recommend that the Overseas Private Investment Corporation's chief information officer document a separation-of-duties matrix for* [redacted] *user roles and responsibilities.*

~~(SBU)~~ ***Recommendation 3.*** *We recommend that the Overseas Private Investment Corporation's chief information officer implement a written process to recertify* [redacted] *accounts annually, including evaluating the separation of duties.*

~~(SBU)~~ Recommendation 4. *We recommend that the Overseas Private Investment Corporation's chief information officer implement a written process to disable inactive [redacted] accounts.*

~~(SBU)~~ Recommendation 5. *We recommend that the Overseas Private Investment Corporation's chief information officer [redacted]*

~~(SBU)~~ Recommendation 6. *We recommend that the Overseas Private Investment Corporation's chief information officer either (1) [redacted] and document the results, or (2) document acceptance of the [redacted]*

Recommendation 7. *We recommend that the Overseas Private Investment Corporation's chief information officer document and implement asset management procedures, including inventorying information system assets on an organization-defined frequency.*

~~(SBU)~~ Recommendation 8. *We recommend that the Overseas Private Investment Corporation's chief information officer document and implement a separation-of-duties matrix for [redacted] user roles and responsibilities.*

Recommendation 9. *We recommend that the Overseas Private Investment Corporation's chief information security officer, in coordination with the security officer, document and implement physical and environmental security policies and procedures including reviews of physical access as defined by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."*

Recommendation 10. *We recommend that the Overseas Private Investment Corporation's chief information officer document and implement an enterprise architecture methodology in line with the Federal enterprise architecture and risk management framework.*

Recommendation 11. *We recommend that the Overseas Private Investment Corporation's chief information officer update the Corporation's incident response plan to include the time frames for reporting incidents as specified in the "United States Computer Emergency Readiness Team Federal Incident Notification Guidelines."*

Recommendation 12. *We recommend that the Overseas Private Investment Corporation's chief information officer complete the implementation of the Training Management System and verify in writing that records are retained for the Corporation-specified period.*

Recommendation 13. *We recommend that the Overseas Private Investment Corporation's chief information officer implement a documented process to validate whether the annual testing of the Corporation's information system contingency plan is completed.*

~~(SBU)~~ Recommendation 14. *We recommend that the Overseas Private Investment Corporation's chief information officer document and implement processes to achieve acceptable compliance with configuration baseline settings for* [redacted]

Recommendation 15. *We recommend that the Overseas Private Investment Corporation's chief information officer implement the process to validate whether plans of action and milestones are completed and updated on time and document the results.*

~~(SBU)~~ Recommendation 16. *We recommend that the Overseas Private Investment Corporation's chief information security officer review the accreditation boundaries of the OPIC* [redacted]*, align external services with related mission functions, and document the results.*

Recommendation 17. *We recommend that the Overseas Private Investment Corporation's chief information security officer implement a written process to assess external services before their authorizations to operate expire.*

In finalizing the report, Clifton evaluated OPIC's responses to Recommendations 1 through 17 contained in the draft report. Both Clifton and OIG acknowledge OPIC's management decisions on all 17 recommendations.

Thank you for your cooperation and the courtesies extended to our staff and Clifton's employees during the engagement.

Sincerely,

/s/

Alvin A. Brown
Deputy Assistant Inspector General for Audit

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

Final Report

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.cliftonlarsonallen.com

TABLE OF CONTENTS

SUMMARY OF RESULTS

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

The act also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology are mandatory for Federal agencies.

The USAID Office of Inspector General engaged us, CliftonLarsonAllen LLP (CLA), 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 minimum security controls for selected information systems in support of FISMA.

Our audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

~~(SBU)~~ For this audit, we reviewed all of OPIC's systems: [redacted]

Results

The audit concluded that OPIC implemented 84 of 105 selected security controls for selected information systems in support of FISMA. For example, OPIC complied with the following requirements:

- Implemented effective audit log monitoring, review and analysis.

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

- 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.

Although OPIC had policies for its information security program, its implementation of those policies was not always fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. The audit found that OPIC had not effectively implemented 21 of 105 selected security controls and identified the following actions that OPIC needed to take to correct the weaknesses in its information security program:

- ~~(SBU)~~ Strengthen [redacted] surrounding patch and configuration management.

- Periodically review network accounts and strengthen account management controls.

- ~~(SBU)~~ Strengthen [redacted] account management.

- [redacted] ~~(SBU)~~ [redacted]

- ~~(SBU)~~ Strengthen authorization processes and security control assessments for [redacted]

- ~~(SBU)~~ Strengthen [redacted] controls.

- Strengthen OPIC asset management controls.

- ~~(SBU)~~ Strengthen [redacted] separation of duties controls.

- Strengthen physical and environmental controls.

- Strengthen enterprise architecture controls.

- Update the incident response plan.

- Maintain training and rules of behavior records.

- ~~(SBU)~~ Test the [redacted] contingency plan.

- Strengthen compliance of baseline configurations.

- Strengthen plan of action and milestones processes.

- ~~(SBU)~~ Assess [redacted] components.

We have made 17 recommendations to assist OPIC in strengthening its information security program. (See pages 3 – 20) In response to the draft report, OPIC outlined its plans to address all 17 recommendations. Based on our evaluation of management comments, we acknowledge management decisions on all recommendations. OPIC's comments are included in their entirety in Appendix II.

Detailed findings appear in the following section.

AUDIT FINDINGS

1. ~~(SBU)~~ Strengthen [redacted] Surrounding Patch and Configuration Management

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control RA-5, states the agency is responsible for the following:

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

~~(SBU)~~ Independent network scans noted [redacted] related to patch management and configuration management. Many of the patch management vulnerabilities [redacted] significant efforts in remediating the most vulnerable hosts and most risky vulnerabilities. OPIC management stated that the overall risk scoring was reduced by half from December 2015 to April 2016. Remaining known vulnerabilities were in process of remediation based on the largest risk reduction for the enterprise.

Unmitigated vulnerabilities on the OPIC 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.
- Agency employees may be unable to access systems.
- Agency data may be lost, stolen or used for nefarious means.

As a result, we recommend the following.

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

2. Periodically Review Network Accounts and Strengthen Account Management Controls

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

> The organization manages information system accounts, including:
>
> * * *
>
> h. Notifies account managers:
>
> 1. When accounts are no longer required
>
> * * *
>
> j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]

In addition, the *Overseas Private Investment Corporation OCIO/Information Security, Access Control Procedure*, Security Control section "(AC-2) Account Management Procedures and Guidelines," states:

> The following procedure provides guidance for the management of accounts on OPIC information systems. This includes account creation, auditing, modifying and disabling.
>
> * * *
>
> e. The System Owner ensures that temporary and emergency accounts are properly authorized and maintained. These accounts are automatically disabled in accordance with OPIC policy as defined in the OPIC 800-53 Parameters.

Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters, security control AC-2, requires review of system and service accounts semi-annually and disabling of accounts based on outcome of review.

~~(SBU)~~ In fiscal year 2015, OPIC [redacted] were not reviewed as part of a [redacted] as required by OPIC policies and procedures. After identification, OPIC management [redacted]. Management indicated that the [redacted] were not included as part of the recertification process prior to identification. OPIC acknowledged that they had not fully implemented their process to recertify OPIC [redacted] and they were refining it during each annual review. In addition, management indicated that they plan to include [redacted] in the fiscal year 2015 account review.

~~(SBU)~~ In fiscal year 2016, OPIC still was not including recertification of [redacted] as part of the annual recertification process. OPIC management indicated that the infrastructure support team performing the recertification was continuing to work through the accounts; however, [redacted]

~~(SBU)~~ By not performing periodic recertification of [redacted], there is an increased risk of unauthorized privileged access to critical systems. Not disabling inactive or unnecessary accounts, including [redacted], also increases the risk of unauthorized access to the system.

A recommendation addressing this finding was issued in the fiscal year 2015 audit.[2] At the end of audit fieldwork, OPIC provided final corrective action to implement a documented process for reviewing service accounts. Therefore, we are not making a recommendation at this time.

3. ~~(SBU)~~ Strengthen [redacted] Account Management Controls

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

> The organization manages information system accounts, including:
> * * *
> h. Notifies account managers:
> 1. When accounts are no longer required
> * * *
> i. Authorizes access to the information system based on:
> 1. A valid access authorization;
> * * *
> j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]

In addition, security control AC-5, states the following regarding separation of duties:

> The organization:
> a. Separates [*Assignment: organization-defined duties of individuals*];
> b. Documents separation of duties of individuals; and
> c. Defines information system access authorizations to support separation of duties.

In addition, the *Overseas Private Investment Corporation OCIO/Information Security, Access Control Procedure*, Security Control section "(AC-5) Separation of duties," states:

> 1) System Owners shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

~~**(SBU)**~~ In fiscal year 2015, the [redacted] reported that management did not have a separation of duties matrix or account recertification for the [redacted] In February of 2015, OPIC management proactively identified a need for a matrix to identify conflicting roles and responsibilities

[2] Recommendation 1, *Audit of the Overseas Private Investment Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, as Amended* (Audit Report No. A-OPC-15-009-P, September 17, 2015).

and an enhancement request to the design. However, as of May 2016, the matrix had not been created or implemented. In addition, OPIC had not performed account recertification for [redacted] during fiscal year 2016.

~~(SBU)~~ Additionally, [redacted] one of a sample of eight did not have an access request form in place. Furthermore, [redacted] were marked as active; however, the accounts had not been used within 90 days but remained active.

The separation of duties matrix enhancement request had received a priority level of medium; therefore, higher priorities were being addressed first. In addition, the user recertification did not occur due to other business process changes taking priority. OPIC did not have a process in place to review accounts that were inactive. OPIC management indicated that they expect a working solution in June of 2016.

~~(SBU)~~ By not performing periodic recertification and separating duties of [redacted], there is an increased risk of unauthorized privileged access to critical systems. Not disabling inactive or unnecessary accounts also increases the risk of unauthorized access to the system. Therefore, we are making the following recommendations.

> ~~(SBU)~~ ***Recommendation 2:*** *We recommend that the Overseas Private Investment Corporation Chief Information Officer document a separation of duties matrix for* [redacted] *user roles and responsibilities.*
>
> ~~(SBU)~~ ***Recommendation 3:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a written process to recertify* [redacted] *accounts annually to include evaluation of separation of duties.*
>
> ~~(SBU)~~ ***Recommendation 4:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a written process to disable inactive* [redacted] *accounts.*

4. ~~(SBU)~~ [redacted]

~~(SBU)~~ According to [redacted]

~~(SBU)~~ In fiscal year 2015, OPIC [redacted]

[redacted] This is due to the [redacted]

~~(SBU)~~ In fiscal year 2016, the [redacted]

~~(SBU)~~ By [redacted] there is an increased [redacted] information system and/or the information system data. Therefore, we are making the following recommendation to address this weakness.

~~(SBU)~~ ***Recommendation 5:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement* [redacted]

5. ~~(SBU)~~ Improve System Security Authorization Processes and Security Control Assessments for [redacted]

NIST Special Publication 800-53, Revision 4, security control CA-2, states the following regarding Security Assessments:

> The organization:
> b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

[3] ~~(SBU)~~ [redacted]

In addition, the *Overseas Private Investment Corporation OCIO/Information Security, Security Assessment and Authorization Policy*, states the following regarding (CA-2):

> OPIC shall assess the security controls of information systems as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing and evaluation of the information system as part of the system development life cycle process.

Furthermore, the policy states the following regarding (CA-6) Security Authorization:

> System Owners shall ensure that their systems are certified and accredited at their initial operating capability, annually, and whenever a significant change occurs.

~~**(SBU)**~~ OPIC's [redacted], had an Authorization to Operate that expired April 22, 2015. The reauthorization of the system was dependent on the Security Assessment, which was conducted during the course of the fiscal year 2016 FISMA audit. However, over a year had lapsed since the last assessment was completed in April 2014. The assessment was delayed due to infrastructure changes that were completed in December of 2015. OPIC management completed the [redacted] re-authorization on May 20, 2016.

Without a completed security assessment and Authorization to Operate, senior level agency officials may not make fully informed decisions regarding risks to the system and its operation. Since OPIC addressed the issue during the audit, a recommendation will not be made at this time.

6. Implementation of Citrix Could be Strengthened

NIST Special Publication 800-53, Revision 4, security control SC-7, states the following regarding boundary protection:

> Control Enhancement:
>
> 7) The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

~~**(SBU)**~~ OPIC's [redacted] were not configured to [redacted] from communicating information to and from the Citrix environment. OPIC allowed Citrix connections from [redacted]. Information was capable of being written and saved to and from [redacted]. This occurred because OPIC did not configure [redacted] OPIC management indicated that [redacted] may prevent testing required to leverage [redacted]

~~(SBU)~~ Not restricting the capability to [redacted] may introduce [redacted] Therefore, we are making the following recommendation.

> ~~(SBU)~~ ***Recommendation 6:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer either (1)* [redacted] *and document the results or (2) document acceptance of the risk of* [redacted]

7. Strengthen Asset Management Controls

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

> The organization:
>
> a. Develops and documents an inventory of information system components that:
>
> 1. Accurately reflects the current information system.
> 2. Includes all components within the authorization boundary of the information system.
>
> 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.
>
> * * *
>
> 5) The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

In addition, the *Overseas Private Investment Corporation Information System Security Policy requires* System Owners to complete the following:

- Develops and documents an inventory of information system components that accurately reflects the current information system; includes all components within the authorization boundary of the information system; is at the level of granularity deemed necessary for tracking and reporting; and includes information deemed necessary to achieve effective information system component accountability as specified in OPIC 800-53 Parameters policy.
- Reviews and updates the information system component inventory as specified in OPIC 800-53 Parameters policy and as an integral part of component installations, removals, and information system updates.

~~(SBU)~~ *Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters*, security control CM-8, requires review and update to the component inventory [redacted]

~~(SBU)~~ OPIC did not conduct [redacted] reviews of their information system inventory as required by OPIC policy. OPIC documented the inventory of its hardware and workstations through [redacted] which monitor [redacted] A master record of the hardware inventory was maintained on [redacted] In addition, management [redacted] However, these methods may [redacted] and may not indicate the current responsible owner.

OPIC recently began removing unused and obsolete inventory. During the removal, OPIC management became aware of devices previously not tracked due to lack of maintaining a detailed component inventory. OPIC management indicated that they recently identified a new asset manager who is working to establish an accurate inventory of hardware and software.

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

> ***Recommendation 7:*** *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.*

8. ~~(SBU)~~ Strengthen [redacted] Separation of Duties Controls

NIST Special Publication 800-53, Revision 4, security control AC-5, states the following regarding separation of duties:

> The organization:
> a. Separates [*Assignment: organization-defined duties of individuals*];
> b. Documents separation of duties of individuals; and
> c. Defines information system access authorizations to support separation of duties.

In addition, the *Overseas Private Investment Corporation OCIO/Information Security, Access Control Procedure*, states the following regarding (AC-5) Separation of Duties:

> System Owners shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or systems access to be able to engage in fraudulent or criminal activity.

~~(SBU)~~ [redacted] In addition, the [redacted] security plan did not

document separation of duties or permissions assigned to different account types. [redacted] was deployed as a new system [redacted] and this control was not defined at the time of deployment. Management was aware of the issue and is currently tracking the issue as part of their plan of action and milestones.

~~(SBU)~~ By not separating duties of [redacted], there is an increased risk of unauthorized privileged access to critical systems. Therefore, we are making the following recommendation.

> ~~(SBU)~~ ***Recommendation 8:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement a separation of duties matrix for* [redacted] *ser roles and responsibilities.*

9. Strengthen Physical and Environmental Controls

NIST Special Publication 800-53, Revision 4, security control PE-1, states the following regarding physical and environmental protection policy and procedures:

> The organization:
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
> 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls

In addition, security control PE-2, states the following regarding physical access authorizations:

> The organization:
> a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
> b. Issues authorization credentials for facility access;
> c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

In addition, security control PE-6, states the following regarding physical access monitoring:

> The organization:
> a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
> b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

c. Coordinates results of reviews and investigations with the organizational incident response capability.

~~(SBU)~~ *Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters*, security controls PE-6 and PE-3, require a [redacted] of physical access logs and an [redacted] of physical access authorizations, respectively.

~~(SBU)~~ OPIC management did not [redacted] of data center access authorizations and [redacted] as required by OPIC's organizational parameters. The primary reason was that OPIC did not have [redacted] Additionally, the OPIC Security Office monitors physical and environmental controls; however, [redacted] During FY 2016, the Chief Information Security Officer and IT security staff were physically relocated within the Security Office to facilitate communication and implementation [redacted]

Without physical and environmental security policies, procedures and access controls in place, the risk of unauthorized individuals gaining access to secure locations is increased. Therefore, we are making the following recommendations.

Recommendation 9: *We recommend that the Overseas Private Investment Corporation's Chief Information Security Officer in coordination with the Security Officer document and implement physical and environmental security policies and procedures including reviews of physical access as defined by National Institute of Standards and Technology Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations.

10. Strengthen Enterprise Architecture Controls

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

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

NIST Special Publication (SP) 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the RMF to Federal information systems including the alignment of security controls the enterprise[4] and security architecture.

[4] Federal Enterprise Architecture Reference Models and Segment and Solution Architectures are defined in the OMB Federal Enterprise Architecture (FEA) Program, FEA Consolidated Reference Model Document, Version 2.3, October 2003 and OMB Federal Segment Architecture

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

The lack of risk management controls for enterprise architecture may increase the difficulty the agency has with managing IT projects and assets. Therefore, we recommend the following.

> ***Recommendation 10:*** *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.

11. Update the Incident Response Plan

NIST Special Publication 800-53, Revision 4, security control IR-8, states the following regarding incident response plans:

> The organization:
> d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

In addition, security control IR-6, states the following regarding incident reporting:

> The organization:
> a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and
> b. Reports security incident information to [Assignment: organization-defined authorities].

Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters, security control IR-6, requires incident-reporting timeframes to be in line with (United States Computer Emergency Readiness Team) US-CERT requirements.

~~(SBU)~~ However, OPIC's Incident Response Plan was not updated to reflect the 2014 *US-CERT Federal Incident Notification Guidelines* regarding threat vectors, impact classifications and notification requirement times. In addition, [redacted]

Methodology (FSAM), January 2009, respectively.

~~(SBU)~~ OPIC management indicated that they were aware of the change in reporting US-CERT requirements; [redacted] OPIC management indicated they will report future incidents in-line with the modified requirements and will update the plan as time permits.

Not reporting incidents timely to US-CERT may prevent the government from accurately correlating threat and attack vector data. This may expose the government agencies to similar unreported incidents. Therefore, we are making the following recommendation.

> ***Recommendation 11:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer update the Incident Response Plan to include the timeframes for reporting incidents as specified in the* United States Computer Emergency Readiness Team Federal Incident Notification Guidelines*.*

12. Maintain Training and Rules of Behavior Records

NIST Special Publication 800-53, Revision 4, security control AT-4, states the following regarding security training records:

> The organization:
>
> a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
> b. Retains individual training records for [Assignment: organization-defined time period].

Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters, security control AT-4, requires training records to be maintained for two years.

Security awareness training records and rules of behavior agreements were not available. Specifically, of the 408 users, for a sample of 25:

- Rules of behavior could not be provided for 17 users.
- Annual Cyber Security Training Evidence could not be provided for 10 users.

In addition, for a sample of 10 of 60 new hires, evidence of privacy training could not be provided for 2 users.

OPIC began using a new Training Management System to track training and could not provide prior records. OPIC management indicated that fiscal year 2016 Cyber Security, Privacy, and Rules of Behavior Training was planned to be completed by June 31, 2016.

Without maintaining accurate training records, OPIC management may not be able to ensure all users are aware of their information security responsibilities. This may result in users disclosing sensitive OPIC information. Therefore, we are making the following recommendation.

Recommendation 12: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer complete the implementation of the Training Management System and verify in writing that records are retained for the corporation-specified period.*

13. ~~(SBU)~~ Test the [redacted] Contingency Plan

NIST Special Publication 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 [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.

Overseas Private Investment Corporation Information System Security Program NIST 800-53 Security Control OPIC Organizational Parameters, security control CP-4, require contingency plan testing annually for moderate systems.

~~(SBU)~~ In 2015, the OPIC [redacted] reported that the [redacted] Information System Contingency Plan (ISCP) was not tested during fiscal year 2015. The [redacted] ISCP was last tested in June of 2014. Therefore, weaknesses identified during the test were not reassessed or new potential issues identified to determine ability to operate in a contingency scenario. OPIC has experienced turnover in personnel that support the ISCP testing. In addition, [redacted] was in process of architectural changes that took priority over testing the as-is state of the system.

OPIC management indicated that ISCP testing was completed in May 2016 as part of the continuity of operations plan testing; however, test results and attendance were not provided. OPIC does not have assurance that such testing was completed. Therefore, we are making the following recommendation.

Recommendation 13: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a documented process to validate whether the annual testing of the information system contingency plan testing is completed.*

14. Strengthen Compliance of Baseline Configurations

NIST Special Publication 800-53, Revision 4, security control CM-6, states the following regarding configuration settings:

> The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

~~**(SBU)**~~ OPIC had documented configuration baselines; however, [redacted] Specifically, the Monthly Executive Report noted [redacted] that exceeded acceptable deviation ranges:

[redacted]

OPIC management indicated that efforts were focused on vulnerability remediation and that benchmark compliance would be the next step. Once OPIC reduces vulnerabilities to a manageable level, the focus will shift more on benchmark compliance.

Without achieving baseline security setting compliance, deployed devices may not have the minimum configuration requirements implemented to protect potential unauthorized access or disclosure of OPIC information. Therefore, we are making the following recommendation.

> ~~**(SBU)**~~ ***Recommendation 14:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement processes to achieve acceptable compliance with configuration baseline settings for* [redacted]

15. Strengthen Plan of Action and Milestones Process

NIST Special Publication 800-53, Revision 4, security control CA-5, states the following regarding plan of action and milestones:

> The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security

controls assessments, security impact analyses, and continuous monitoring activities.

~~(SBU)~~ OPIC's Plan of Action and Milestone (POA&M) included [redacted] where [redacted] In addition, adjusted target completion dates and rationale for why the target date was missed were not included in the POA&M. *OPIC's Security Assessment and Authorization Policy* states that the System Owner will update existing POA&Ms as needed based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OPIC has a process in place to monitor POA&Ms; however, these items were missed during the review and updating of the POA&Ms. The items were overlooked due to prioritization of completing corrective actions rather than updating dates.

Without properly updating POA&Ms to reflect their current status, OPIC is unable to effectively monitor on-going system security risks. As a result, we recommend the following.

> ***Recommendation 15:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement the process to validate whether the plans of action and milestones are completed and updated timely and document the results.*

16. ~~(SBU)~~ Assess [redacted] Components

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

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

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

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

~~(SBU)~~ [redacted] Based on NIST SP 800-18, Revision 1, Section 2.2, a Major Application may consist of multiple individual applications if all are related to a single mission function. [redacted] consists of four individual portfolio mission functions covering [redacted] The four portfolios have individual OPIC authorizations to operate within [redacted] However, the inventory of the external services noted that [redacted] had expired external authorizations to operate (ATOs), outdated information, and incomplete high level Plans of Action and Milestones.

OPIC management indicated that the service provider provides the ATO for each external service. OPIC reviews each external service on a rotational basis every three years, including external ATOs. However, expiring ATOs were not prioritized in the rotational assessment. Therefore, OPIC was not aware of the current security status of external services.

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

> ~~(SBU)~~ ***Recommendation 16:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Security Officer review the accreditation boundaries of the Overseas Private Investment Corporation* [redacted] *and align external services with related mission functions and document the results.*
>
> ***Recommendation 17:*** *We recommend that the Overseas Private Investment Corporation Chief Information Security Officer implement a written process to assess external services before expiration of authorizations to operate.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Overseas Private Investment Corporation (OPIC) outlined its plans to address all 17 recommendations and described planned actions to address the recommendations. OPIC's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on all 17 recommendations.

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether OPIC implemented selected minimum security controls for selected information systems in support on the Federal Information Security Modernization Act of 2014.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4.* We assessed OPIC's performance and compliance with FISMA in the following areas:

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

~~(SBU)~~ For this audit, we reviewed all of OPIC's systems, as follows: [redacted] See Appendix IV for a listing of selected controls for each system. The audit also included a vulnerability assessment of OPIC's [redacted] and an evaluation of OPIC's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit recommendations[5] to determine if OPIC had made progress in implementing the recommended improvements concerning its information security program.

[5] *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.

The audit fieldwork was performed at OPIC's headquarters in Washington, D.C., from March 11, 2016, to June 29, 2016.

Methodology

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

~~(SBU)~~ In addition, we completed a vulnerability assessment of OPIC's [redacted] and evaluated OPIC's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of OPIC vulnerability scanning configurations and network vulnerability scan results and comparing them with independent network vulnerability scan results. We also reviewed the status of the audit recommendations in the fiscal year 2015 FISMA audit report.[6]

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected and if projected may be misleading.

[6] *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.

MANAGEMENT COMMENTS

October 12, 2016

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

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

SUBJECT: OPIC Comments on the Office of the Inspector General's Report Titled *"The Overseas Private Investment Corporation Has Implemented Many Controls in Support of FISMA for Fiscal Year 2016, but Improvements Are Needed"*

Below is the Overseas Private Investment Corporation's response to the Office of Inspector General's (OIG) DRAFT report *"The Overseas Private Investment Corporation Has Implemented Many Controls in Support of FISMA for Fiscal Year 2016, but Improvements Are Needed", with Audit Report Number A-OPIC-16-00XX-P.*

The Inspector General report contains 17 recommendations for corrective action. This memorandum provides OPIC management's response to each recommendation. The Federal Information Security Management Act of 2002 (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 80% (84/105) of the security controls tested. OPIC appreciates the continued support and collaboration with the Inspector General to enhance our cybersecurity program.

Security Controls Surrounding Patch and Configuration Management

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

Management Response:

OPIC values the Inspector General's acknowledgment of the remediation efforts we have applied which have substantially reduced the number and prevalence of the most risky vulnerabilities on our network. Of the remaining known vulnerabilities identified by the OIG's contractor, the Chief Information Officer

will remediate those that may adversely impact OPIC systems. For those vulnerabilities that management chooses not to remediate, the Chief Information Officer will document OPIC's risk acceptance ***by December 31, 2016.***

~~(SBU)~~ [redacted] ***Account Management Controls***

Recommendation No.2: *We recommend that the Overseas Private Investment Corporation Chief Financial Officer document a separation of duties matrix for* [redacted] *user roles and responsibilities.*

~~(SBU)~~***Recommendation No.3:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a written process to recertify* [redacted] *accounts annually to include evaluation of separation of duties.*

~~(SBU)~~ ***Recommendation No.4:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a written process to disable inactive* [redacted].

~~(SBU)~~ **Management Response:**

The Chief Financial Officer will develop a matrix of user roles and responsibilities for [redacted] to ensure separation of duties. In consultation with the Chief Financial Officer, the Chief Information Officer will develop and document a process, which when implemented, will ensure that user accounts are recertified annually for the [redacted] application. Additionally, and in consultation with the Chief Financial Officer, the Chief Information Officer will develop and document a process to disable inactive [redacted] for the [redacted] application. All of the above will be completed **by March 31, 2017.**

~~(SBU)~~ [redacted]

Recommendation No.5: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer* [redacted]

~~(SBU)~~**Management Response:** The Chief Information Officer will ensure that [redacted] OPIC anticipates implementation ***by September 30, 2017***.

Citrix Implementation

~~(SBU)~~ ***Recommendation No.6:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer either (1)* [redacted] *and document the results or (2) document acceptance of the* [redacted]

~~(SBU)~~ **Management Response:** The Chief Information Officer will either [redacted] and document the results, or document the acceptance of the risk of [redacted] ***by January 31, 2017.***

Asset Management Controls

Recommendation No.7: *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.*

Management Response: The Chief Information Officer will improve currently existing asset management policies, procedures, and processes to ensure a comprehensive, accurate, reliable, and timely inventory of information system assets ***by September 30, 2017***.

~~(SBU)~~ [redacted] ***Separation of Duties Controls***

Recommendation No.8: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement a separation of duties matrix for* [redacted] *user roles and responsibilities.*

~~(SBU)~~ **Management Response:** The Chief Information Officer will complete the documentation of user roles in [redacted] to include a separation of duties matrix, and subsequently implement ***by February 28, 2017***.

Physical and Environmental Controls

Recommendation No.9: *We recommend that the Overseas Private Investment Corporation's Security Officer in coordination with the Chief Information Security Officer document and implement physical and environmental security policies and procedures including reviews of physical access as defined by National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.*

Management Response: The OPIC Security Officer, in consultation with Chief Information Security Officer, will document and implement OPIC physical access and environmental security policies and procedures to include reviews of physical access as defined by NIST 800-53, rev 4, and Privacy Controls for Federal Information Systems and Organizations ***by September 30, 2017***.

Enterprise Architecture Controls

Recommendation No. 10: *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.*

Management Response: The OPIC Chief Information Officer will update existing Enterprise Architecture documentation in accordance with Federal Enterprise Architecture and Risk Management Framework and will implement ***by September 30, 2017***.

Incident Response Plan

Recommendation No. 11: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer update the Incident Response Plan to include the timeframes for reporting incidents as specified in the United States Computer Emergency Readiness Team Federal Incident Notification Guidelines.*

Management Response: The OPIC Chief Information Officer will update the OPIC Incident Response Plan to reflect the incident reporting timeframes as specified in the United States Computer Emergency Readiness Team Federal Incident Notification Guidelines ***by November 30, 2016***.

Training and Rules of Behavior

Recommendation No. 12: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer complete the implementation of the Training Management System and verify in writing that records are retained for the corporation-specified period.*

Management Response: OPIC's Training Management System (TMS) now requires all staff to complete mandatory Cybersecurity, Privacy and Rules of Behavior training on an annual basis. The Chief Information Officer, in consultation with OPIC's Senior Records Management Official, will ensure that record of IT training completion for all staff is maintained for a minimum of five (5) years. This action will be documented ***by January 31, 2017***.

~~(SBU)~~ [redacted] ***Contingency Plan***

Recommendation No. 13: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement a documented process to validate whether the annual testing of the information system contingency plan testing is completed.*

Management Response: The Chief Information Officer will implement a documented process to validate annual completion of ISCP testing as defined in OPIC 800-53 organizational parameters ***by March 31, 2017***.

Monitoring of Baseline Configurations

~~(SBU)~~ ***Recommendation No. 14:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Officer document and implement processes to achieve acceptable compliance with configuration baseline settings for* [redacted]

~~(SBU)~~ **Management Response:** The Chief Information Officer will document and implement a process to achieve acceptable compliance with our configuration baseline settings for [redacted] ***by April 30, 2017***.

Plan of Action and Milestone Process

Recommendation No. 15: *We recommend that the Overseas Private Investment Corporation's Chief Information Officer implement the process to validate whether the plans of action and milestones are completed and updated timely.*

Management Response: The Chief Information Officer will update the plans of action and milestones (POA&M) Management Process to ensure all items listed in the plan accurately reflect either completion or all are updated timely to reflect modification to any proposed completion date ***by March 31, 2017***.

External Services Components

~~(SBU)~~ ***Recommendation No. 16:*** *We recommend that the Overseas Private Investment Corporation's Chief Information Security Officer review the accreditation boundaries of the Overseas Private Investment Corporation* [redacted] *and align external services with related mission functions and document the results.*

Recommendation No. 17: *We recommend that the Overseas Private Investment Corporation Chief Information Security Officer implement a written process to assess external services before expiration of authorizations to operate.*

~~(SBU)~~ **Management Response:**
The Chief Information Security Officer will review the accreditation boundaries of the OPIC [redacted] and based on findings, modify OPIC system documents as appropriate ***by September 30, 2017***. The Chief Information Security Officer will also update the OPIC system assessment process to ensure the assessment of external services systems occur on a recurring basis and prior to the expiration of their authorizations to operate ***by May 31, 2017***.

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

Status of Prior Year Findings

The following table provides the status of the FY 2015 FISMA audit recommendations.[7]

~~(SBU)~~			
No.	**FY 2015 Audit Recommendation**	**OPIC Status**	**Auditor's Position on Status**
1	We recommend that the Overseas Private Investment Corporation Chief Information Officer implement a documented process to periodically review [redacted] to determine whether accounts are necessary and disable accounts no longer required.	Closed	Agree, please refer to finding [redacted]
2	We recommend that the Overseas Private Investment Corporation Chief Information Security Officer implement a process to verify all personnel receive security and privacy training annually, and document the results.	Closed	Agree, please refer to finding [redacted] for new finding
3	We recommend that the Overseas Private Investment Corporation Chief Information Security Officer develop and implement documented role-based information technology and security training for personnel.	Closed	Agree
4	We recommend that the Overseas Private Investment Corporation Chief Information Officer implement a documented memorandum of understanding for its [redacted]	Closed	Agree
5	We recommend that the Overseas Private Investment Corporation Chief Information Officer implement a documented interconnection security agreement for its [redacted]	Closed	Agree
6	We recommend that the Overseas Private Investment Corporation's Chief Information Officer [redacted]. If management determines that using such controls are not feasible, document that decision formally and implement mitigating controls.	Closed	Agree, please refer to finding [redacted] for new finding
7	We recommend that the Overseas Private Investment Corporation Chief Information Officer document a risk assessment for [redacted].	Closed	Agree
8	We recommend that the Overseas Private Investment Corporation Chief Information Officer document a system security plan for [redacted]	Closed	Agree
9	We recommend that the Overseas Private Investment Corporation Chief Information Officer complete a security control assessment for [redacted] and document the results.	Closed	Agree
10	We recommend that the Overseas Private Investment Corporation Chief Information Officer document [redacted] authorization to operate based on security assessments and acknowledgement of operating risks.	Closed	Agree

[7] *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.

Summary of Results of Each Control Reviewed

	~~(SBU)~~	
Control	**Control Name**	**Is Control Effective?**
[redacted]		
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	No, See finding [redacted]
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-4	Acquisitions Process	Yes
SA-5	Information System Documentation	Yes
SA-10	Developer Configuration Management	Yes
SA-11	Developer Security Testing and Evaluation	Yes
PS-1	Personnel Security Policy & Procedures	Yes
PS-2	Position Risk Designation	Yes
PS-3	Personnel Screening	Yes
PS-4	Personnel Termination	Yes
PS-5	Personnel Transfer	Yes
PS-6	Access Agreements	Yes
PS-7	Third-Party Personnel Security	Yes
PS-8	Personnel Sanctions	Yes
PE-1	Physical & Environmental Protection Policy and Procedures	No, See finding [redacted]
PE-2	Physical Access Authorizations	No, See finding [redacted]
PE-3	Physical Access Control	Yes
PE-4	Access Control for Transmission Medium	Yes
PE-5	Access Control for Output Devices	Yes
PE-6	Monitoring Physical Access	No, See finding [redacted]
PE-8	Visitor Access Records	Yes
PE-9	Power Equipment & Cabling	Yes
PE-10	Emergency Shutoff	Yes
PE-11	Emergency Power	Yes
PE-12	Emergency Lighting	Yes
PE-13	Fire Protection	Yes
PE-14	Temperature & Humidity Controls	Yes
PE-15	Water Damage Protection	Yes
PE-16	Delivery & Removal	Yes
PE-17	Alternate Work Site	Yes

	~~(SBU)~~	
Control	**Control Name**	**Is Control Effective?**
PE-18	Location of Information System Components	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	Yes
CP-3	Contingency Training	Yes
CP-4	Contingency Plan Testing and Exercises	No, See finding [redacted]
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes
CP-8	Telecommunication Services	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
CM-1	Configuration Management Policy & Procedures	Yes
CM-2	Baseline Configuration	Yes
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	No, See finding [redacted]
CM-7	Least functionality	Yes
CM-8	Information System Component Inventory	No, See finding [redacted]
SI-2	Flaw remediation	Yes
IR-1	Incident Response Policy & Procedures	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	No, See finding [redacted]
IR-8	Incident Response Plan	No, See finding [redacted]
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	Yes
AT-3	Role-Based Security Training	Yes
AT-4	Security Training Records	No, See finding [redacted]
IA-1	Identification & Authentication Policy and Procedures	Yes
IA-2	Identification & Authentication (Organizational Users)	No, See finding [redacted]
IA-3	Device Identification & Authentication	Yes
IA-4	Identifier Management	Yes
IA-5	Authenticator Management	Yes
AC-1	Access Control Policy & Procedures	Yes
AC-2	Account Management	No, See finding [redacted]
AC-3	Access Enforcement	Yes
AC-4	Information Flow Enforcement	Yes
AC-5	Separation of Duties	Yes
AC-6	Least Privilege	Yes
AC-11	Session Lock	Yes
AC-17	Remote Access	Yes

	~~(SBU)~~	
Control	**Control Name**	**Is Control Effective?**
AC-19	Access Control for Mobile Devices	Yes
AU-6	Audit, Review, Analysis and Reporting	Yes
SC-7	Boundary Protection	No, See finding [redacted]
SC-8	Transmission Integrity	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	No, See finding [redacted]
CA-3	System Interconnections	Yes
CA-5	Plan of Action and Milestones	No, See finding [redacted]
CA-6	Security Authorization	No, See finding [redacted]
CA-7	Continuous Monitoring	Yes
PM-1	Information Security Program Plan	Yes
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	Yes
PM-5	Information System Inventory	Yes
PM-6	Information Security Measures of Performance	Yes
PM-7	Enterprise Architecture	No, See finding [redacted]
PM-8	Critical Infrastructure Plan	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes
[redacted]		
SA-9	External Information System Services	Yes
AC-2	Account Management	No, See finding [redacted]
AC-5	Separation of Duties	No, See finding [redacted]
AC-6	Least Privilege	Yes
AC-20	Use of External Information Systems	Yes
[redacted]		
SA-9	External Information System Services	Yes
AC-20	Use of External Information Systems	Yes
CA-6	Security Authorization	No, See finding [redacted]
CA-7	Continuous Monitoring	Yes
[redacted]		
SA-9	External Information System Services	Yes
AC-2	Account Management	Yes
AC-5	Separation of Duties	No, See finding [redacted]
AC-6	Least Privilege	Yes
AC-20	Use of External Information Systems	Yes

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
oig.usaid.gov
Task Number AA101016