OFFICE OF INSPECTOR GENERAL

AUDIT OF THE OVERSEAS PRIVATE INVESTMENT CORPORATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, AS AMENDED FOR FISCAL YEAR 2015

AUDIT REPORT NO. A-OPC-15-009-P
SEPTEMBER 17, 2015

WASHINGTON, D.C.

This is our summary report on the *Audit of the Overseas Private Investment Corporation's Fiscal Year 2015 Compliance With the Federal Information Security Management Act for 2002, as Amended* (Audit Report No. A-OPC-15-009-P). The Federal Information Security Management Act of 2002 (FISMA), as amended, 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 source. The act also requires agencies to have an annual assessment of their information systems.

The USAID Office of Inspector General (OIG) contracted with CliftonLarsonAllen LLP (Clifton) to conduct the audit. According to Clifton officials, they performed this audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. The objective was to determine whether the Overseas Private Investment Corporation (OPIC) implemented selected security and privacy controls for selected information systems in support of FISMA, as amended.

To answer the audit objective, Clifton assessed whether OPIC implemented 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*. Clifton performed audit fieldwork at OPIC's headquarters in Washington, D.C., from April 29 to July 30, 2015.

The audit concluded that OPIC implemented 96 of 101 selected security and privacy controls for selected information systems in support of FISMA, as amended. For example, OPIC complied with the following requirements:

- Categorized its information systems and the information processed, stored, or transmitted in them in accordance with federal guidelines, and designated senior officials to review and approve the security categorizations.

- Implemented an effective program for incident handling and response.

- Implemented contingency planning and recovery controls.

- Implemented a policy and procedures for change management.

However, OPIC did not implement five controls designed to preserve the confidentiality, integrity, and availability of its information and information systems. OIG made ten recommendations based on Clifton's report to assist OPIC in strengthening its information security program. OIG also acknowledged OPIC's management decisions on all the recommendations.

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
http://oig.usaid.gov
Audit Task No. AA100515