OFFICE OF INSPECTOR GENERAL

AUDIT OF THE OVERSEAS PRIVATE INVESTMENT CORPORATION'S FISCAL YEAR 2014 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

AUDIT REPORT NO. A-OPC-14-007-P
SEPTEMBER 11, 2014

WASHINGTON, D.C.

This is our summary report on the "Audit of the Overseas Private Investment Corporation's Fiscal Year 2014 Compliance With the Federal Information Security Management Act of 2002" (Audit Report No. A-OPC-14-007-P). The Federal Information Security Management Act of 2002 (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 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 in accordance with U.S. Government auditing standards. The objective was to determine whether the Overseas Private Investment Corporation (OPIC) implemented selected security controls for selected information systems in support of FISMA.

To answer the audit objective, Clifton assessed whether OPIC implemented 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. Clifton performed audit fieldwork at OPIC's headquarters in Washington, D.C., from June 4 through July 17, 2014.

The audit concluded that OPIC implemented 74 of 78 selected security controls in support of FISMA. For example, OPIC did the following:

- 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 an effective incident handling and response program.

- Maintained an effective specialized training program for employees who need role-based training.

- Established appropriate segregation of duties within OPICNet, the corporation's general support system.

Clifton concluded that, although OPIC generally had policies for its information security program, its implementation of those policies was not always effective enough to preserve the confidentiality, integrity, and availability of the corporation's information and information systems. Based on Clifton's report, OIG made six recommendations to help OPIC strengthen its information security program and one to address a weakness in the recommendation closure process. Management decisions were made on all seven 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