OFFICE OF INSPECTOR GENERAL

AUDIT OF THE MILLENNIUM CHALLENGE CORPORATION'S FISCAL YEAR 2013 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

AUDIT REPORT NO. M-000-13-005-P
SEPTEMBER 20, 2013

WASHINGTON, D.C.

This is a summary of our report on the "Audit of the Millennium Challenge Corporation's Fiscal Year 2013 Compliance With the Federal Information Security Management Act of 2002." The Office of Inspector General (OIG) contracted the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the audit in accordance with generally accepted government auditing standards.

The objective of the audit was to determine whether the Millennium Challenge Corporation (MCC) implemented selected minimum security controls for selected information systems to meet the Federal Information Security Management Act of 2002 (FISMA) requirements to reduce the risk of data tampering, unauthorized access to and disclosure of sensitive information, and disruption to MCC's operations.

To answer the audit objective, Clifton assessed whether MCC implemented selected management, technical, and operational controls outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Revision 3. Clifton performed audit fieldwork at MCC's headquarters in Washington, D.C., from March 28, 2013, to July 11, 2013.

The audit concluded that MCC implemented 116 of 141 selected security controls for selected information systems in support of FISMA. For example, MCC complied with the following NIST requirements:

- 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 adequate and effective specialized training program for employees who needed role-based training.

- Implemented an effective identification and authentication program.

- Implemented an effective system maintenance program.

Although MCC generally had policies for its information security program, its implementation of those policies 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.

To address the weaknesses reported in Clifton's report, OIG made 15 recommendations to MCC's management. Four of them asked MCC to reopen recommendations made in the previous year's audit. Although OIG acknowledged MCC management decisions on each of the 15 recommendations, it did not agree with MCC's management decisions for 2. Therefore, OIG encouraged MCC to revisit its management decisions for those recommendations and revise them to fully address the weaknesses identified in Clifton's audit report.

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