OFFICE OF INSPECTOR GENERAL

AUDIT OF THE MILLENNIUM CHALLENGE CORPORATION'S FISCAL YEAR 2015 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, AS AMENDED

AUDIT REPORT NO. A-MCC-16-001-P
October 26, 2015

WASHINGTON, D.C.

This is a summary of our report on *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002,*[1] *as amended* (No. A-MCC-16-001-P).[2] The act, referred to as 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 Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the audit. Clifton was required to conduct the audit in accordance with U.S. government auditing standards. The objective was to determine whether the Millennium Challenge Corporation (MCC) implemented selected minimum security and privacy controls for selected information systems in support of FISMA, as amended.

To answer the audit objective, Clifton assessed whether MCC implemented selected 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 MCC's headquarters in Washington, D.C., from March 16, 2015, through July 23, 2015.

The audit concluded that MCC implemented 105 of 115 selected security and privacy controls for selected information systems in support of FISMA, as amended. For example, MCC complied with requirements by doing the following:

- Implementing an effective incident handling and response program.
- Maintaining an adequate, effective specialized training program for its employees requiring role-based training.
- Implementing an effective identification and authentication[3] program.
- Establishing a media sanitization program.
- Implementing an enterprise architecture strategy.

Although MCC generally had policies for its information security program, Clifton found that MCC's implementation of those policies 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.

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 added a new subchapter on information security to the United States Code at 44 USC 3541-3549.

[2] 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.

[3] According to the National Institute of Standards and Technology, identification and authentication is "the process of verifying the identity of a user, process, or device," which is usually performed before allowing access to resources in an information technology system.

Consequently, the audit identified areas in the information security program that MCC can improve.

Based on Clifton's report, OIG made eight recommendations to help MCC strengthen its information security program. Clifton and OIG acknowledge MCC's management decisions on all 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
www.usaid.gov/oig
Audit Task No. AM100215