OFFICE OF INSPECTOR GENERAL

AUDIT OF THE MILLENNIUM CHALLENGE CORPORATION'S FISCAL YEAR 2014 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

WASHINGTON, DC

This is a summary of our report on the *Audit of the Millennium Challenge Corporation's Fiscal Year 2014 Compliance With the Federal Information Security Management Act of 2002* (Report No. A-MCC-14-008-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 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 controls for selected information systems in support of FISMA.

To answer the audit objective, Clifton assessed whether MCC implemented selected management, technical, and operational controls outlined in National Institute of Standards and Technology 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 12 through June 27, 2014.

The audit concluded that MCC implemented 104 of 116 selected security controls for selected information systems in support of FISMA. For example, MCC complied with requirements by doing the following:

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

- Implemented an effective incident handling and response program.

- Maintained an adequate and effective specialized training program for its employees requiring role-based training.

- Implemented an effective identification and authentication program.

- Established appropriate segregation of duties in MCCNet, a general support system through which all MCC systems interact and communicate.

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 Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, and destruction. The audit identified areas in the information security program that MCC could improve. Accordingly, OIG made seven recommendations to help MCC strengthen its information security program. After reviewing Clifton's evaluation of management comments and the documentation provided by MCC, we acknowledge management decisions on all recommendations and final action on Recommendation 7.

---

[*] National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, took effect during the audit. Because it did not significantly change the findings, Clifton used Revision 4.