Federal Information Security Management Act: **Fiscal Year 2014 Evaluation (ISD-IN-MOA-0005-2014)**

The Federal Information Security Management Act (FISMA) (Public Law 107-347) requires Federal agencies to have an annual independent evaluation of their information security programs and practices performed by their Office of Inspector General or by an independent external auditor, as determined by their OIG, to determine the effectiveness of such programs and practices. KPMG LLP (KPMG), an independent public accounting firm, performed Department of Interior's FISMA evaluation for fiscal year (FY) 2014, under a contract issued by DOI and monitored by OIG.

For FY 2014, KPMG adopted a risk-based approach and reviewed a sample of 14 Department and contractor information systems at 7 bureaus and offices. Specifically, KPMG reviewed information security practices, policies, and procedures at:

- Bureau of Indian Affairs;
- Bureau of Land Management;
- Bureau of Reclamation;
- U.S. Fish and Wildlife Service;
- Interior Business Center;
- Office Of The Secretary; and
- Office of the Special Trustee for American Indians.

KPMG concluded that, consistent with applicable FISMA requirements, Office of Management and Budget policy, and National Institute of Standards and Technology guidelines, DOI has established and maintained security programs for continuous monitoring management, incident and response reporting, plan of action and milestones, remote access management, contractor systems, and security capital planning.

KPMG identified needed improvements, however, in maintaining the configuration management, identity and access management, risk management, contingency planning, and security training program areas. Moreover, KPMG made seven recommendations intended to strengthen DOI's information security program.

As part of our oversight of KPMG's FISMA activities, we—

- reviewed KPMG's approach and planning of the audit;
- evaluated the auditors' qualifications and independence;
- monitored the audit's progress at key milestones;
- engaged in regularly scheduled meetings with KPMG and DOI management to discuss audit progress, findings, and recommendations;
- reviewed KPMG's supporting work papers and audit report; and
- performed other procedures as deemed necessary.

KPMG is responsible for the findings and conclusions expressed in its evaluation report. We did not express an opinion on the report or on KPMG's conclusions regarding DOI's compliance

with relevant laws and regulations. We referred KPMG's recommendations to the Department's Office of Financial Management for audit follow-up.

The evaluation report contains DOI Information Technology/Internal Systems Data that is considered Sensitive but Unclassified and therefore not routinely released under the Freedom of Information Act (FOIA). To submit a FOIA request, see DOI's FOIA program online(http://www.doi.gov//foia/index.cfm).