Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2025 (Report No. 2025-CTD-016)

Objectives

The objectives of this performance audit were to:

1. Determine whether the U.S. Department of the Interior's (DOI's) overall information security program and practices were consistent with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA).[1]

2. Complete the U.S. Department of Homeland Security (DHS) fiscal year (FY) 2025 CyberScope reporting metrics.[2]

Background

FISMA requires Federal agencies to have performed an annual independent evaluation of their information security programs and practices to determine the effectiveness of such programs and practices. This evaluation is to be performed by the agency's Office of Inspector General (OIG) or, at the OIG's discretion, by an independent external auditor.

Audit Approach

KPMG, an independent public accounting firm, performed DOI's FY 2025 FISMA performance audit under a contract issued by DOI and monitored by our office. As required by the contract, KPMG asserted that it conducted the audit in accordance with generally accepted government auditing standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG reviewed information security practices, policies, and procedures at the following six DOI bureaus and offices:

- Bureau of Land Management
- U.S. Fish and Wildlife Service
- Bureau of Reclamation
- Office of the Chief Information Officer
- Office of the Secretary
- U.S. Geological Survey

To ensure the quality of the performance audit work, we:

- Reviewed KPMG's approach and audit planning.
- Evaluated the auditors' qualifications and independence.
- Monitored the audit's progress at key milestones.
- Met regularly with KPMG and DOI management to discuss audit progress, findings, and recommendations.

[1] Pub. L. No. 113-283.

[2] CyberScope, operated by DHS on behalf of the Office of Management and Budget (OMB), is a web-based application designed to streamline IT security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, offices of inspectors general (OIGs) provide an independent assessment of effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

- Reviewed KPMG's supporting work papers and audit report.
- Performed other procedures as deemed necessary.

Public Release

FISMA reporting has been completed in accordance with Office of Management and Budget (OMB) Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements,* dated January 15, 2025. We are publicly releasing a summary of the report rather than the full report itself because FISMA requires OIGs to take appropriate steps to ensure the protection of information that, if disclosed, may adversely affect information security.[3]

Results

Based on the results of KPMG's performance audit procedures, all six of the Cybersecurity Functions assessed were lower than Level 4: Managed and Measurable.[4] Therefore, the information security program was not considered effective according to the instructions detailed within the 2025 IG FISMA Reporting Metrics Guidance. Using OMB's guidance and the CyberScope results, KPMG determined the calculated average of the Cybersecurity Functions were assessed as Consistently Implemented (Level 3). We do not express an opinion on the report or on KPMG's conclusions regarding DOI's compliance with laws and regulations.

Recommendations

KPMG identified needed improvements in cybersecurity governance, risk and asset management, configuration management, identity and access management, security training, and contingency planning. KPMG made 18 recommendations related to control deficiencies identified during its performance audit that, if effectively implemented by DOI, should strengthen DOI's information security program. Furthermore, KPMG stated that DOI should implement a robust monitoring capability to continually assess the cybersecurity state of its information systems, including a process to hold bureaus and offices accountable for identified control deficiencies. In response to the draft report, the Office of the Chief Information Officer concurred with all recommendations and established a target completion date for each corrective action.

Followup

We will track the Office of the Chief Information Officer's implementation of KPMG's recommendations. The legislation creating the OIG requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement recommendations; and recommendations that have not been implemented.

[3] FISMA § 3555, "Annual independent evaluation."

[4] FISMA metrics are aligned to six functions: Govern, Identify, Protect, Detect, Respond, and Recover. The information security program is then assessed using a maturity model spectrum scored on five levels: Level 1, "Ad-hoc"; Level 2, "Defined"; Level 3, "Consistently Implemented"; Level 4, "Managed and Measurable"; and Level 5, "Optimized."