Summary: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2022 (Report No. 2022–ITA–028)

Objective

The objectives of this 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) 2022 CyberScope reporting metrics.[2]

Background

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

Audit Approach

KPMG, an independent public accounting firm, performed the DOI's FY 2022 FISMA audit under a contract issued by the 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 DOI's Office of the Chief Information Officer and the following 11 DOI bureaus and offices:[3]

- Bureau of Indian Affairs
- Bureau of Land Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement

[1] Pub. L. No. 113–283.

[2] CyberScope, operated by the DHS on behalf of the Office of Management and Budget, 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 provide an independent assessment of effectiveness of an agency's information security program. Offices of inspectors general must also report their results to the DHS and the Office of Management and Budget annually through CyberScope.

[3] The OIG has a unique status within the DOI. Pursuant to the Inspector General Act of 1978, we have specific authorities and the capacity (and obligation) to act independently on a range of issues, and we have dual reporting obligations to both the DOI Secretary and to Congress. Currently, however, we have made the decision to share infrastructure with the DOI for compatibility and access to departmental data and resources. Because we rely on some aspects of the DOI's IT infrastructure, we considered the OIG's performance with respect to the issues covered in this report.

- U.S. Fish and Wildlife Service
- National Park Service
- Office of Inspector General
- Office of the Secretary
- Office of Surface Mining Reclamation and Enforcement
- Office of the Solicitor
- U.S. Geological Survey

To ensure the quality of the 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.
- 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–22–05, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements,* dated December 6, 2021. 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.[4]

Results

Based on the maturity levels calculated in CyberScope, KPMG determined DOI's information security program was not effective because it was not consistent with applicable FISMA requirements, OMB policy and guidance, or National Institute of Standards and Technology standards and guidelines. According to the OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines,* a security program is considered effective if most of the FY 2022 Core Inspector General Metrics are at least Level 4, "Managed and Measurable."[5] Using the OMB's guidance and the CyberScope results, KPMG determined that most of the cybersecurity functions were Level 3, "Consistently Implemented." KPMG is responsible for the findings and

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

[5] FISMA metrics are aligned to five functions: 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."

conclusions expressed in the audit report. We do not express an opinion on the report or on KPMG's conclusions regarding the DOI's compliance with laws and regulations.

Recommendations

KPMG identified needed improvements in the areas of risk management, supply chain risk management, identity and access management, configuration management, data protection and privacy, information security continuous monitoring, incident response, and contingency planning. KPMG made 24 recommendations related to these control weaknesses intended to strengthen the DOI's information security program as well as those of the bureaus and offices. In its 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 refer KPMG's recommendations to the Office of Financial Management for audit followup. 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.