Audit of the Drug Enforcement Administration's
Spider Core System Pursuant to the
Federal Information Security Modernization
Act of 2014, Fiscal Year 2021

★ ★ ★

22-051

MARCH 2022

Audit of the Drug Enforcement Administration's Spider Core System Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2021

Objectives

The objectives of this audit were to determine whether the Drug Enforcement Administration's (DEA) Spider Core system security program and practices were consistent with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA). In addition, the audit was designed to perform a vulnerability assessment of the Spider Core system and evaluate selected system security controls.

Results in Brief

The audit identified a weakness in one of the two control areas that need to be strengthened to ensure that DEA's Spider Core system and data are adequately protected. In addition, we identified control deficiencies in three of the nine domain areas and one of the eight Congressional Letter areas of the DEA's Information Security Program. Those findings and subsequent recommendations are reported in the Audit of the DEA's Information Security Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2021.

Recommendations

This audit provides four recommendations for improving the DEA Spider Core system.

To ensure DEA was immediately aware of the deficiencies identified during this audit, the auditors presented the finding to DEA management prior to the issuance of this report. DEA management concurred with the identified weakness.

Public Release

The Department of Justice (DOJ) Office of the Inspector General (OIG) is publicly releasing this Commentary and Summary of the report rather than the full report itself because Inspectors General are required by FISMA to take appropriate steps to ensure the protection of information that, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk.

Audit Approach

KPMG LLP conducted this performance audit of the DEA Spider Core system under the direction of the DOJ OIG and in accordance with Generally Accepted Government Auditing Standards (GAGAS) and the Office of Management and Budget (OMB) reporting requirements. The OIG reviewed KPMG LLP's report and related documentation for compliance with GAGAS. The OIG's review was not intended to enable the OIG to make a conclusion about the effectiveness of DEA's information security controls. KPMG LLP is responsible for the attached auditors' report dated October 29, 2021, and the conclusions expressed in the report. The OIG's review disclosed no instances where KPMG LLP did not comply, in all material respects, with GAGAS and OMB reporting requirements.

Background

FISMA was passed by Congress and signed into law by the President in 2014. FISMA assigns responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and OMB to strengthen federal information system security. This includes directing NIST to develop standards and guidelines for ensuring the effectiveness of information security controls over information systems that support federal agencies' operations and assets, and requiring the head of each agency to implement policies and procedures to cost-effectively reduce risks to an acceptable level.

Annually, agency Inspectors General are required to either perform an independent evaluation or contract an independent external auditor to perform an evaluation of the agency's information security program and practices to ensure the effectiveness of the program and practices. Each evaluation must include: (1) testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; (2) an assessment (based on the results of the testing) of compliance with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems.