# Audit of the Federal Bureau of Investigation's Information Security Management Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2024

★ ★ ★

AUDIT DIVISION

25-020

JANUARY 2025

# COMMENTARY AND SUMMARY

**Audit of the Federal Bureau of Investigation's Information Security Management Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2024**

## Objectives

The objectives of this audit were to: (1) determine whether the Federal Bureau of Investigation's (FBI) overall information security management program and practices were consistent with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA); (2) examine areas and vulnerabilities requested by the U.S. House of Representatives Committee on Oversight and Reform; and (3) determine whether the FBI took action in response to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Binding Operational Directive 23-01. The OIG audits FBI's compliance with FISMA and other appropriate criteria each fiscal year (FY).

## Results in Brief

The audit identified weaknesses in six of the nine FISMA domain areas that need to be strengthened to ensure that FBI's information systems and data are adequately protected. In addition, the audit verified that FBI continued to have vulnerabilities related to 15 recommendations issued in prior audits.

## Recommendations

This audit provides 15 new recommendations for improving FBI's information security management program, and 15 prior recommendations issued to the FBI from FY 2021 through FY 2023 remain open. To ensure the FBI was immediately aware of the findings identified during this audit, the auditors presented the findings to FBI management prior to the issuance of this report. FBI management concurred with the identified weaknesses.

## 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 FBI's information security management program 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 FBI's information security controls. KPMG LLP is responsible for the attached auditors' report dated September 27, 2024, 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.