



Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



**Audit of the Federal Bureau of
Investigation's Information Security
Program Pursuant to the Federal
Information Security Modernization
Act of 2014
Fiscal Year 2017**



Commentary and Summary

Audit of the Federal Bureau of Investigation's Information Security Program Pursuant to the Federal Information Security Modernization Act of 2014 Fiscal Year 2017

Objectives

The objectives of this audit were to determine whether the Federal Bureau of Investigation's (FBI) overall information security program and practices were consistent with the requirements of the Federal Information Security Modernization Act (FISMA). In addition, the audit was designed to complete the Department of Homeland Security FY 2017 Cyberscope reporting metrics.

Results in Brief

The audit identified weaknesses in six of the seven domain areas in FBI's information security program (ISP) that need to be strengthened to ensure that FBI's information systems and data are adequately protected.

Recommendations

This audit provides 38 recommendations for improving FBI's ISP.

To ensure FBI was immediately aware of the deficiencies 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 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 (KPMG) conducted this performance audit of the FBI's ISP under the direction of the Department of Justice Office of the Inspector General (OIG) and in accordance with U.S. Generally Accepted Government Auditing Standards (GAGAS) and the Office of Management and Budget (OMB) reporting requirements. The OIG reviewed KPMG'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 the FBI's information security controls. KPMG is responsible for the attached auditors' report dated October 12, 2017, and the conclusions expressed in the report. However, the OIG's review disclosed no instances where KPMG 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 ISP 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 system.



The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL

950 Pennsylvania Avenue, Northwest
Suite 4760
Washington, DC 20530-0001

Website
oig.justice.gov

Twitter
[@JusticeOIG](https://twitter.com/JusticeOIG)

YouTube
[JusticeOIG](https://www.youtube.com/JusticeOIG)

Also at Oversight.gov