Audit of the Justice Management Division's Security Controls and the Personnel Accountability and Assessment System (PAAS) 2.0 Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2025

★ ★ ★

AUDIT DIVISION

26-026

February 2026

COMMENTARY AND SUMMARY

Audit of the Justice Management Division's Security Controls and the Personnel Accountability and Assessment System (PAAS) 2.0 Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2025

Objectives

The objectives of this audit were to: (1) determine whether the Justice Management Division's (JMD) information security control policies, procedures, practices, and facilities were consistent with the requirements of National Institute of Standards and Technology (NIST) and, as related to a selection of field sites; (2) determine whether the JMD has taken action in response to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Binding Operational Directive (BOD) 23-01. This included examining select security policies and procedures within the Personnel Accountability and Assessment System (PAAS) 2.0 system for compliance with NIST 800-53 security controls. In addition, a vulnerability assessment of PAAS 2.0 was performed.

Results in Brief

The audit identified weaknesses in the control areas of PAAS 2.0 that resulted in findings. These findings are in addition to the findings identified in JMD's Information Security Management Program; those findings and associated recommendations are reported separately in the Audit of the JMD's Information Security Management Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2025.

Recommendations

This audit provides two recommendations for improving certain controls for JMD's PAAS 2.0 system.

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 PAAS 2.0 under the direction of the DOJ OIG and in accordance with Generally Accepted Government Auditing Standards (GAGAS) and 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 JMD's information security controls. KPMG LLP is responsible for the attached auditors' report dated September 30, 2025, 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.