DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

FOR IMMEDIATE RELEASE
June 16, 2026

DOJ OIG Releases Report on the Audit of the Department of Justice Information System Inventory Management

Department of Justice (DOJ) Assistant Inspector General Performing the Duties of the Inspector General M. Sean O'Neill announced today the release of a report evaluating information technology (IT) inventory management practices at the Justice Management Division (JMD), the Executive Office for U.S. Attorneys (EOUSA), and the U.S. Marshals Service (USMS). DOJ's ability to safeguard its unclassified information systems from cybersecurity threats depends on having full visibility into and a complete and accurate inventory of those systems.

The DOJ Office of the Inspector General's (OIG) audit found that while DOJ has established policies and procedures to record information systems in its Joint Cybersecurity Authorization Management application (JCAM), deficiencies exist in inventory recordkeeping and privacy assessment processes that can hinder DOJ's ability to ensure data accuracy and system compliance.

The OIG's specific findings included:

- **Recordkeeping Practices Should be Improved.** JCAM users at JMD, EOUSA, and USMS demonstrated inconsistent and non-compliant recordkeeping practices, leading to incomplete and outdated inventory records. While most deficiencies were minor, two systems were improperly categorized as non-Federal Information Security Modernization Act-reportable, potentially delaying required security measures and oversight.
- **DOJ Policies Lack Regular Inventory Validation.** DOJ does not routinely validate and certify its information systems inventory for completeness and accuracy, which is essential for accurate records, compliance, and cybersecurity. The last full certification by DOJ components occurred in March 2023 following a USMS cybersecurity breach.

- **DOJ Needs to Improve the Timeliness of Privacy Assessment Approvals.** Over half of the sampled component inventory records did not contain required privacy documentation, raising concerns about privacy risk mitigation in system operations. We confirmed that some missing privacy assessments remained under review at the Office of Privacy and Civil Liberties (OPCL) and were delayed for months or years. OPCL attributed these delays to the components' understaffing, staff turnover, and challenges in addressing OPCL comments and revisions. These delays suggest components may operate systems with inadequate privacy safeguards.

The OIG made five recommendations to improve DOJ's IT inventory management practices and ensure the inventory data is complete and accurate. JMD and OPCL agreed with all five recommendations.

Report: Today's report is available on the OIG's website.

Please contact us at OIG.Media@usdoj.gov if you have any questions.

###