# Audit of the Department of Justice's Information System Inventory Management

★ ★ ★

AUDIT DIVISION

26-064

June 2026

# EXECUTIVE SUMMARY

## Audit of the Department of Justice's Information System Inventory Management

### Objective

Our objective was to determine whether the Department of Justice's information technology (IT) inventory management practices ensured a complete and accurate accounting of its unclassified IT systems. Maintaining an inventory of IT systems is critical to the Department's ability to safeguard them against malicious unauthorized access, use, disclosure, disruption, modification, and damage. Our audit scope generally covered the policies and procedures for managing information system inventories at the Justice Management Division (JMD), the Executive Office for U.S. Attorneys (EOUSA), and the U.S. Marshals Service (USMS).

### Results in Brief

The Department's ability to safeguard its information systems from cybersecurity threats depends on Department IT security subject matter experts having full visibility of those systems. A 2023 ransomware attack on a USMS information system operating outside of the Department's cybersecurity oversight highlighted gaps in this area.

Our audit found that the Department's inventory management repository provides components with a critical tool to account for all information systems. However, we found that the Department's disjointed inventory policies and lack of inventory data entry standards have led to inconsistent and often non-compliant recordkeeping practices, and inconsistent, incomplete, and outdated inventory records. Additionally, the Department does not regularly validate all information systems in its inventory to ensure completeness and accuracy. Further, over half of the sampled component inventory records we examined lacked required privacy documentation, raising concerns about the mitigation of privacy risks in system operations.

### Recommendations

Our report contains five recommendations to improve the Department's IT inventory management practices and ensure the inventory data is complete and accurate. JMD and the Office of Privacy and Civil Liberties (OPCL) concurred with our recommendations in response to a draft of this report; the response can be found in Appendix 2. Our analysis of JMD's and OPCL's response and actions needed to close the report can be found in Appendix 3.

### Audit Results

The Department requires all components to record their IT inventories in the Joint Cybersecurity Authorization Management application (JCAM), which includes system information and supporting documentation describing security and privacy controls applied to the system. JCAM also supports compliance with regulatory requirements such as the Federal Information Security Modernization Act (FISMA) and privacy assessment approvals. As of November 2025, JCAM contained records for nearly 1,000 unclassified information systems in operation across all DOJ components.

#### Recordkeeping Practices Should be Improved to Ensure Consistency, Reliability, and Transparency of the Department's Inventory Data

JCAM users at JMD, EOUSA, and the USMS employed varying and often non-compliant recordkeeping practices for their inventory data, resulting in inconsistent, incomplete, and outdated inventory records. We believe this was due to disjointed inventory policies and a lack of JCAM data entry standards.

Additionally, the absence of documentation requirements for special system categorizations, such as those related to FISMA requirements, prevents the Department from independently validating these determinations in JCAM.

Our audit identified two systems that were not properly categorized as FISMA-reportable—an error that could delay the implementation of mandated security protections and critical oversight, and increase risk to the systems themselves.

We also found that the Department's IT inventory management policies and procedures are scattered across multiple guides and policies, and no single DOJ policy document consolidates all the recordkeeping requirements related to IT inventory management. This fragmented approach increases the risk of non-compliance with, inconsistent application of, and reduced confidence in the reliability of JCAM inventory records.

### Performing Regular Inventory Validation Assures Completeness and Accuracy

DOJ policies lack regular reporting or validation of the completeness and accuracy of the Department's full inventory of information systems. While components are required to perform quarterly validations of information systems meeting FISMA reportability thresholds, this process excludes over 60 percent of the Department's information systems. Notably, the last time DOJ components certified the completeness and accuracy of their full inventory of information systems occurred in early 2023, prompted by a ransomware attack on a USMS information system.

Regular inventory validation is critical to maintaining accurate records, ensuring all information systems are captured in JCAM, helping to ensure compliance with statutory, regulatory, and DOJ requirements, and, ultimately, ensuring the security of the Department's systems and data against cyber threats.

### The Department Needs to Improve the Timeliness of Privacy Assessment Approvals

The Department relies on JCAM to document privacy assessments, a critical process overseen by OPCL. Privacy assessments are conducted to identify and mitigate potential privacy risks for information systems processing Personally Identifiable Information (PII) and must be approved by OPCL before initiating an information system.

We found that JCAM records for multiple information systems lacked documentation of the completed privacy assessments prior to the initiation of the system. This raises concerns that components may be operating systems with inadequate privacy risk mitigation measures.

# Table of Contents

# Introduction

Information Technology (IT) plays an important and powerful role in advancing, protecting, and serving the Department of Justice's (DOJ or Department) mission, which relies on a complex network of IT systems to execute its law enforcement, litigation, incarceration, civil protection, and national security mandates. The prominence and nature of the Department's mission and responsibilities also make its IT systems regular targets for cyber attacks. Consequently, full visibility by IT security personnel into IT systems across over 40 DOJ components is essential to fortifying the Department's cybersecurity posture, and maintaining an inventory of its IT systems is critical to safeguarding against the malicious unauthorized access, use, disclosure, disruption, modification, and damage of those systems. To this end, the Federal Information Security Modernization Act (FISMA) requires federal agency heads to maintain an inventory of information systems operated by their agencies.[1]

The importance of managing information systems to address and mitigate security risks was demonstrated in February 2023, when a ransomware attack on a U.S. Marshals Service (USMS) system exposed the consequences of inadequate system visibility. The breached system, which contained 15 terabytes of sensitive law enforcement data and personally identifiable information (PII), operated outside the Department's cybersecurity oversight, and the attack resulted in the theft of over 140 gigabytes of data and rendered most of the system inaccessible to USMS users. According to the Department's report to Congress about the incident, following the breach, the Department discovered that USMS leadership had allowed the system to bypass agency IT governance policies for over a decade. This incident demonstrated how even a single non-compliant system can represent a significant cybersecurity risk—particularly if it is not cataloged and governed within the larger enterprise inventory.

In March 2023, in the wake of the USMS breach, the Deputy Attorney General (DAG) issued a memorandum requiring all DOJ component heads to certify the accuracy of their IT inventory records. The effort identified 10 components with previously unrecorded information systems, underscoring the importance of performing regular inventory validations to maintain visibility of all information systems operating within the Department.[2]

## DOJ IT Inventory Management and Oversight

The Office of the Chief Information Officer (OCIO) in the Justice Management Division leads the Department's efforts to mitigate cybersecurity risks. OCIO oversees enterprise-wide IT governance, including policy setting, capital planning and investment control, enterprise architecture, and—most relevant to this audit—maintaining the Department's IT system inventory. This stewardship enables senior leadership to make informed decisions on budgeting, resource allocation, risk management, system modernization, and strategic planning, while ensuring compliance with regulatory requirements like FISMA.

---

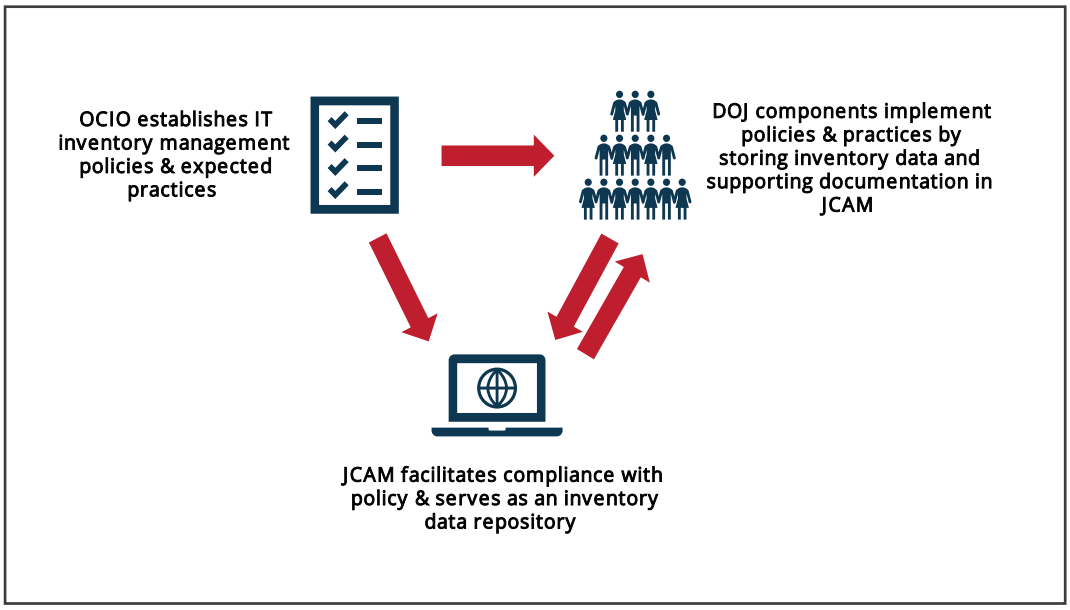
[1] FISMA (Pub. L. No. 113-283).

[2] Although the DOJ Office of the Inspector General (OIG) was one of the DOJ components responsible for responding to the 2023 DAG memorandum, we excluded the OIG from the scope of this audit to comply with federal auditing and independence standards. Appendix 1 includes a detailed explanation of this audit's objectives, scope, and methodology.

IT management and oversight responsibilities within OCIO are divided among three staff offices, covering all aspects of IT management, including cybersecurity policy and guidance, and compliance across the Department. OCIO manages the Joint Cybersecurity Authorization Management (JCAM) application, the Department's official repository for data on information systems.[3] JCAM stores system information and supporting documentation which detail each system's planning, implementation, and validation of security and privacy controls. The Department also uses JCAM to ensure systems comply with FISMA requirements. Figure 1 illustrates how the Department leverages JCAM to manage its IT inventory. As of November 2025, JCAM contained records for 980 operational, unclassified information systems, subsystems, and applications used across DOJ components.

Figure 1

DOJ Information System Inventory Management in JCAM




Source: OIG

OCIO uses tools like zero-trust architecture and system scanning to manage cybersecurity risks for systems in JCAM. These tools authenticate users, control access to systems, detect vulnerabilities, and monitor unusual activity on the DOJ network. OCIO also monitors cybersecurity risks through its Security Posture Dashboard Report, an automated tool that analyzes scan results to provide a near real-time, holistic view of the Department's cybersecurity posture, and enabling stakeholders to identify and prioritize risks. Because JCAM's effectiveness relies on the integrity of the data entered, DOJ components must ensure all systems are included and that data entered is complete and accurate.

[3] In 2023, the Department renamed its Cyber Security Assessment and Management system to JCAM.

## OIG Audit Approach

The objective of this audit was to determine whether the Department's IT inventory management practices ensured a complete and accurate accounting of its IT systems. Our audit reviewed the Department's policies and procedures for managing its inventory of unclassified information systems, focusing on practices at the Justice Management Division (JMD), the Executive Office for U.S. Attorneys (EOUSA), and the USMS. JMD was selected for its cybersecurity oversight and enterprise system management role, EOUSA for its litigating function, and the USMS for its law enforcement role and to evaluate its response to the 2023 cybersecurity incident. To accomplish our objective, we:

- Interviewed Department officials and analyzed inventory records from JMD, EOUSA, and the USMS.
- Evaluated the sampled DOJ components' compliance with IT system inventory management policies.
- Tested the completeness and accuracy of a judgmental sample of system records in JCAM, including 17 JMD systems, 9 EOUSA systems, and 16 USMS systems, all in various stages of system life cycle.[4]

Appendix 1 contains further details on our audit objective, scope, and methodology, including a list of sampled systems.

[4] As of November 2025, JMD had 129 operational information systems in its inventory, EOUSA had 86 systems, and the USMS had 45 systems.

# Audit Results

The Department's use of JCAM provides DOJ components with a critical tool to account for their information systems and maintain complete and accurate inventory records. However, we identified inconsistencies in the inventory data in JCAM, including varying level of detail about each system and inconsistent supporting documentation. These issues stem from disjointed IT inventory management policies and the absence of clear data entry standards specifying what information should be recorded in JCAM, how it should be documented, and when updates should occur. Consequently, for the systems we tested, JCAM inventory records often contained incomplete, unsupported, outdated, and pre-decisional information, undermining their reliability and value to Department and component leadership. Enhancing these IT inventory management policies to address these deficiencies will help the Department improve data accuracy and consistency, streamline workflows, and support informed decision-making.

## Recordkeeping Practices Should be Improved to Ensure Completeness and Accuracy of the Department's IT Inventory Data

JCAM users at JMD, EOUSA, and the USMS employ inconsistent and often non-compliant recordkeeping practices for maintaining their JCAM inventory data, resulting in inconsistent, incomplete, and outdated inventory records that hinder the Department's ability to verify and validate the completeness and accuracy of its IT inventory. In conducting our work, we selected a risk-based sample of operational information systems belonging to JMD, EOUSA, and the USMS. Specifically, we examined JCAM records for 11 JMD systems, 6 EOUSA systems, and 4 USMS systems.[5] Some records for these systems in JCAM were incomplete and missing documentation required by DOJ policy. We believe this occurred because the Department's IT inventory management policies do not clearly define required information or provide DOJ components with adequate guidance.

### Lack of JCAM Data Entry Standards

The DOJ Security Privacy Assessment and Authorization Handbook (SPAA) directs Department IT staff to secure, manage, and report on DOJ information systems and requires all components to document information systems in JCAM. DOJ components must submit a JCAM registration form to OCIO for each information system, detailing its name, classification, operational status, function, processed information type, applicable categorizations such as FISMA reportability, and whether the system supports critical elements of a component's mission.

The SPAA specifies information and supporting documentation required in the JCAM record. However, it lacks detailed guidance on document format, storage location, update schedules, or templates available to streamline preparation and approval. In addition to the SPAA, the DOJ IT Governance Guide establishes procedures, practices, and guidelines governing how DOJ information systems must be managed and grants program managers discretion in tailoring system documentation for their assigned projects. The IT Governance Guide also establishes a component self-governance program for managing agency-specific IT

[5] In addition, we included in our sample an additional 10 USMS information systems to assess compliance with privacy assessment requirements only, as discussed below.

investments. Similarly, OCIO expects components to manage their own systems with minimal oversight from JMD.

However, the lack of detailed JCAM guidance, coupled with the latitude granted to components to self-manage their IT inventory, created an environment conducive to inconsistent recordkeeping and the existence of non-compliant JCAM records with incomplete, missing, outdated, unsupported, and pre-decisional information. Of the 21 operational information systems we sampled, only one fully complied with JCAM record requirements. We determined that many of the deficiencies were not significant; however, 11 of the sampled system JCAM records were missing approved privacy documentation validating whether the system processes PII, which we discuss in further detail later in this report.

Each inventory record in JCAM contains several pages that users populate with information about the system. While JCAM allows users to link supporting documentation to specific pages for better organization and to facilitate compliance with DOJ policy, this is not required. We found that the sampled components occasionally failed to name and link system documents consistently, making it difficult to locate support for the inventory data. Without document linkages, users must rely on JCAM's search function to locate them, which can be cumbersome and error prone due to misspellings, ambiguous filenames, and the inclusion of outdated documents, duplicate uploads, or files with broken links. This further complicates efforts to determine if data is current or accurate. These deficiencies undermine the reliability of JCAM as a tool for managing the Department's IT inventory, creating inefficiencies and increasing the risk of non-compliance with DOJ policies.

Establishing standardized data entry requirements for components to follow in maintaining inventory records in JCAM, including document linkages, file naming conventions, and update schedules, will likely improve operational efficiency, reduce errors, and facilitate compliance. Without such requirements, JCAM data may continue to be unreliable, potentially misleading Department leaders, component heads, and other oversight bodies responsible for informed decision making. Therefore, to ensure consistency, accuracy, and usability of JCAM records, we recommend that JMD establish clear data entry standards, including supporting document linkages, file naming conventions, and update schedules for the system inventory data stored in JCAM.

## Accurate and Verifiable System Categorizations Ensure Proper Protection, Accountability, and Oversight

Accurate system categorizations are essential to ensure appropriate security, oversight, and monitoring of DOJ information systems. The SPAA requires the JCAM record to indicate whether a system has received a special designation, including mission essential, critical infrastructure, or high-value asset. The Department prioritizes protection of systems with these designations, making accurate categorization critical. While most JCAM records included these special categorizations, we were unable to verify their accuracy due to the lack of Department policy requiring components to document support for these determinations.

**Special System Categorizations**

**Mission Essential** – Critical communication and information systems that directly support DOJ-identified Mission Essential Functions.

**Critical Infrastructure** – A system so vital to the United States that its incapacity or destruction would have a debilitating impact on national security or public health.

**High Value Asset** – An information system deemed of high value to US government operations or a high-value target to US adversaries.

The JCAM record should also contain an appropriate designation related to FISMA reportability. FISMA establishes a statutory government-wide cybersecurity framework requiring federal agencies to inventory, categorize, secure, and continuously monitor their information systems. It mandates security protections for systems handling federal data, proportional to the risk and potential magnitude of the harm of a cybersecurity incident. Without accurate system categorization, protections are not put in place, potentially putting federal operations, data, and missions at risk. Additionally, because FISMA requires agency Inspectors General to evaluate the agency's information security annually to ensure the effectiveness of the program and practices, accurate identification of FISMA-reportable information systems is essential to defining the scope of oversight and compliance verification performed via OIG audits and ensuring all relevant systems are included in the Department's quarterly FISMA inventory.

The SPAA establishes criteria for DOJ components to determine FISMA reportability, including whether systems are mission essential, critical infrastructure, or high value assets; or whether they process PII. The SPAA also allows authorized officials to make informed, risk-based decisions when determining FISMA reportability; however, it does not require DOJ components to document their rationale for the decision, limiting the ability of stakeholders—including those responsible for ensuring the security and compliance of Department systems—to verify the appropriateness of these determinations.

For our sample of systems, we tested the accuracy of the Department's FISMA reportability determinations by applying SPAA criteria to JCAM system data. We identified four systems that we initially believed met FISMA-reportable criteria but were not categorized as such.[6] Though two of these systems from JMD processed PII, OCIO determined they did not warrant FISMA-reportable categorization. However, this rationale was not included in the JCAM records for either system. As for the other two systems—one each from EOUSA and the USMS—after we brought these two systems to the attention of OCIO officials, those

[6] The OIG previously identified deficiencies in FISMA reportability determinations. In November 2021 during the OIG's Audit of the Department's Cyber Supply Chain Risk Management Effort, Report Number 22-087 (July 2022), EOUSA reexamined its information systems and identified 21 additional FISMA-reportable systems, underscoring the need for transparency and oversight of special system categorizations. https://oig.justice.gov/sites/default/files/reports/22-087.pdf

officials agreed that the systems were incorrectly categorized, confirmed that EOUSA had made the necessary correction for its system, and coordinated with the USMS to correct the other system's categorization in JCAM. OCIO officials also agreed that additional controls over FISMA reportability determinations would be beneficial to improve accuracy.

Requiring documentation of special system categorizations, including FISMA reportability, will likely improve operational efficiency and oversight by enabling leadership to independently validate these determinations in JCAM, helping to ensure that mandated security protections are implemented, and helping to ensure that the systems are subject to the oversight processes required of FISMA-reportable systems, including those of the OIG. We therefore recommend that JMD establish requirements to document justifications for special system categorizations in JCAM, such as FISMA reportability, mission essential systems, critical infrastructure, and high value assets.

### Synchronized and Consolidated Inventory Recordkeeping Policies May Reduce Risk of Noncompliance

FISMA requires the Department to establish policy and standards for managing the security and privacy of its information systems. While OCIO maintains an online library of policies, job aids, cybersecurity guides, rules of behavior, and templates, we noted that this library lacks a JCAM user guide. Instead, the Department's IT inventory management policies and procedures are scattered across at least six separate guides and policies, including the SPAA, the IT Governance Guide, the Plan of Action and Milestones (POA&M) Guide, the Information System Contingency Planning (ISCP) Guide, and privacy assessment guidance from the DOJ Office of Privacy and Civil Liberties (OPCL). As shown in Table 1, we found that no single DOJ policy or guidance document consolidates all the recordkeeping requirements related to IT inventory management. Furthermore, not all the recordkeeping requirements listed in Table 1 are required to be maintained in JCAM.

Table 1

Location of DOJ IT Inventory Recordkeeping Requirements

| Recordkeeping Requirement[a] | DOJ Policy or Guidance Source | | | | | |
|---|---|---|---|---|---|---|
| | SPAA | IT Governance Guide | POA&M Guide | ISCP Guide | JCAM Registration Form | OPCL Guidance |
| Basic System Information & Description | X | | | | X | |
| System Security & Privacy Plan | X | | | | | |
| Plan of Action and Milestones (POA&M) | | | X | | | |
| Authorization Boundary Diagram | X | | | | | |
| Privacy Assessments | X | X | | | | X |
| JCAM System Registration Form | X | | | | X | |
| Records & Information Management Certification | X | X | | | | |
| DOJ Identity & Authentication Risk Assessment | X | | | | | |
| Business Case Analysis | | X | | X | | |
| Information System Contingency Plan Documentation | | X | | X | | |
| IT Staff Training Completion | | | | X | | |
| Security Assessment & Authorization Compliance | | X | | | | |
| Supply Chain Risk Review | | X | | | | |
| System Design Document | | X | | | | |

[a] This is not an exhaustive list of the Department's IT inventory recordkeeping requirements.

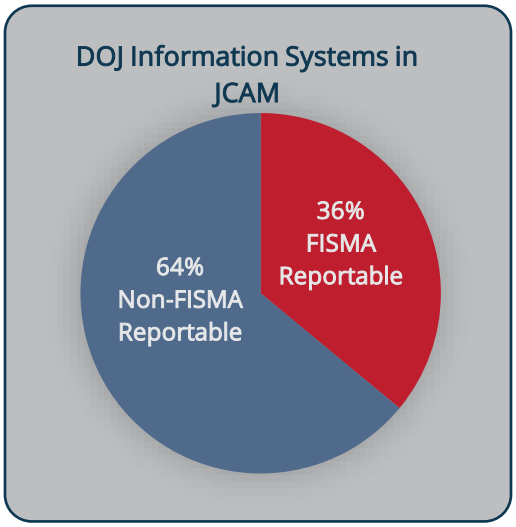
Source: OIG

In our judgment, this fragmentation contributes to the inconsistent recordkeeping practices we observed in JCAM. Staff may be unaware of certain requirements, particularly requirements that appear in policies with which they are less familiar. This lack of clarity weakens accountability, complicates oversight, and increases the risk of non-compliance, which ultimately leads to a less secure cyber environment. It also reduces operational efficiency by complicating training, onboarding, and policy updates, while potentially undermining stakeholder confidence in the reliability of JCAM inventory records. As a result, we recommend that JMD consolidate IT inventory recordkeeping guidance to ensure consistent management and maintenance of information system data across all components.

## Performing Regular Inventory Validation Assures Completeness and Accuracy

DOJ policies do not require regular validation of the completeness and accuracy of the Department's entire information systems inventory. For FISMA-reportable IT systems, the Department receives inventory validations from components through quarterly FISMA Chief Information Officer (CIO) metrics data call submissions, as required by DOJ Order 0904. These metrics, issued annually by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), guide federal agencies in reporting their cybersecurity activities. OCIO coordinates the Department's response by obtaining a list of FISMA-reportable systems from JCAM and distributing it to DOJ components for responses. According to an OCIO official, only components with FISMA-reportable systems are required to respond to the CISA-related data call. Our review of the Department's April 2025 data call response found that it largely excluded non-FISMA-reportable information systems.[7]

Information systems designated as non-FISMA reportable are excluded from the submissions and thus not validated. This is significant, as FISMA reportable systems comprise only 36 percent of the Department's information systems inventory in JCAM. The Department is exposed to increased risk with 64 percent of its IT systems potentially unverified in JCAM. Since the quarterly FISMA inventory process excludes non-FISMA-reportable systems, the Department does not have a process to periodically validate the completeness and accuracy of its full information systems inventory. Furthermore, we found little evidence in our sampled system records that components are performing regular validations of their inventory data. Without a comprehensive inventory validation process, the Department has limited assurance that components maintain complete and accurate IT system inventory records.




Source: JCAM

Our audit identified two best practices in the Department that we believe could serve as potential models for Department-wide improvements in the area of periodic inventory validations. First, the USMS has a monthly process requiring that information system security officers and system owners meet to review the security status of their assigned information systems and to verify inventory data accuracy. This process involves completing a 17-task checklist, including verifying and updating JCAM records, system categorizations, privacy and contingency planning documentation, and the system description. The completed checklist must be signed and uploaded into JCAM, ensuring transparency and confidence in the system's security posture. A USMS information system security officer stated that the checklists are a useful tool for facilitating communication with system owners and monitoring changes to the information systems. In our judgment, this validation process offers an effective way to maintain accurate information system inventory records.

Second, the March 2023 inventory effort, directed by the DAG in response to the USMS breach, was the last time DOJ components certified the completeness and accuracy of their full inventory of information

[7] The Department's April 2025 FISMA CIO metrics data call response included 354 FISMA-reportable systems and 3 non-FISMA-reportable systems.

systems. According to an OCIO official, components took the memorandum seriously and responded accordingly. In April 2023, OCIO reported the results of the system inventory effort to the DAG, outlining component responses to seven action areas, providing OCIO visibility into the Department's adherence to various DOJ cybersecurity metrics, and as previously mentioned, identified several previously unrecorded information systems, which were subsequently entered into JCAM. An OCIO official told us the 2023 inventory was a one-time event.

In our judgment, regular review of the Department's IT inventory records ensures all information systems are captured in JCAM and enables OCIO to properly oversee DOJ components' compliance with statutory, regulatory, and DOJ requirements, and ultimately strengthens the Department's cybersecurity posture. As a result, we recommend that JMD develop and implement a plan for performing regular inventory validations across all DOJ information systems. This plan should consider existing best practices, including the USMS monthly validation process, to ensure JCAM records for each system are complete and accurate.

## The Department Needs to Improve the Timeliness of Privacy Assessment Approvals

The Department uses JCAM not only to document the IT inventory, but also to contribute to its management of certain privacy-related requirements overseen by the Office of Privacy and Civil Liberties (OPCL). OPCL ensures Department components comply with laws, regulations, and policies protecting privacy. To facilitate compliance, OPCL reviews components' preliminary determination of whether an information system collects, processes, or transmits PII, and provides guidance and templates for preparing Initial Privacy Assessments (IPA) and Privacy Impact Assessments (PIA), both of which, if required, must be uploaded into JCAM.

An IPA is the first step in the Department's process to identify and mitigate potential privacy risks and should be completed early in the design, development, or significant modification of any information system processing PII. The IPA helps components assess the need for additional privacy protections and determines if a PIA is required. OPCL reviews and approves IPAs, issuing a formal legal determination outlining any additional privacy requirements for the system. Components must upload IPA final determinations into JCAM.

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA before developing, procuring, or initiating information systems that collect, maintain, or disseminate PII. PIAs identify and assess privacy risks and mitigation for Department information systems collecting PII. OPCL reviews and approves completed PIAs and components must upload final PIAs into JCAM.

Among the 21 information systems in our initial sample, we found that required privacy assessments were missing for 10 systems. We then expanded our sample size to include 10 additional systems and found that, in total, the JCAM records for 17 systems owned by JMD, EOUSA, and the USMS did not include required privacy assessments. The missing assessments included 9 IPA final determinations and 8 PIAs.[8] While some of these missing assessments were still in the process of being drafted and had not yet been submitted to OPCL, 10 (or 59 percent) of the 17 missing assessments were at the OPCL review stage, where OPCL and components collaborate on further edits or clarifications necessary for OPCL to finalize and approve the

[8] For one of its systems, EOUSA had neglected to upload the IPA final determination into JCAM and corrected the record after we brought the issue to its attention.

assessment. Notably, we found that all non-compliant systems were operational, raising concerns that these systems were operating without adequate privacy risk mitigation measures.

In evaluating the causes of the delays to the IPAs and PIAs, we confirmed that some assessments had been at the review stage for months or years. OPCL officials attributed some of the delays to: (1) understaffing and turnover among privacy and IT personnel at the components leading to difficulty in components' ability to respond to OPCL comments and proposed edits; and (2) repeated revisions between components and OPCL to resolve issues. OPCL officials stated that, to expedite the privacy review process, they have provided additional privacy training to components, as they believe a lack of understanding of privacy requirements by component privacy and IT staff contributes to inaccurate privacy document submittals. The OPCL officials also told us they have delegated additional approval authority to OPCL attorneys to address the portion of the backlog attributable to OPCL.

Delays in reviewing and approving privacy documentation can hinder system development, procurement, or operation of Department information systems, and if those systems are launched without appropriate privacy reviews, the delays can potentially result in inadequate protection of PII. As a result, we recommend that OPCL evaluate the privacy workflow process and collaborate with components to streamline the IPA and PIA review, approval, and documentation processes to ensure timely completion of privacy assessments.

# Conclusion and Recommendations

Maintaining a complete and accurate inventory of all Department information systems, with all necessary supporting information, is critical for the effective monitoring of and protection against cybersecurity threats. While we found that the Department had established policies and procedures to capture information systems in JCAM, we also identified deficiencies in inventory recordkeeping and privacy assessment processes that hindered its ability to ensure data accuracy and system compliance. Strengthening JCAM data-entry requirements, consolidating inventory guidance, and implementing regular inventory validations will enhance the completeness, accuracy, and utility of JCAM data for decision-making. Furthermore, streamlining the privacy workflow process to expedite reviews and approvals will help ensure timely completion of privacy assessments and reduce risks to PII. Addressing these gaps will bolster the Department's ability to comply with statutory and regulatory requirements, and ultimately to safeguard its systems and data.

To achieve that end, we recommend that JMD:

1. Establish clear data entry standards, including supporting document linkages, file naming conventions, and update schedules for the system inventory data stored in JCAM.

2. Establish requirements to document justifications for special system categorizations in JCAM, such as FISMA reportability, mission essential systems, critical infrastructure, and high value assets.

3. Consolidate IT inventory recordkeeping guidance to ensure consistent management and maintenance of information system data across all components.

4. Develop and implement a plan for performing regular inventory validations across all DOJ information systems. The plan should consider existing best practices, including the USMS monthly validation process, to ensure JCAM records for each system are complete and accurate.

We also recommend that OPCL:

5. Evaluate the privacy workflow process and collaborate with components to streamline the IPA and PIA review, approval, and documentation processes to ensure timely completion of privacy assessments.

# APPENDIX 1: Objective, Scope, and Methodology

## Objective

The objective of this audit was to determine whether the Department's information technology (IT) inventory management practices ensured a complete and accurate accounting of its IT systems.

## Scope and Methodology

We evaluated the IT inventory management policies and procedures at JMD, EOUSA, and the USMS, focusing on each component's recordkeeping practices in JCAM and JMD's oversight of components' IT inventory management. To accomplish our objective, we examined Department and component-level processes for ensuring that all information systems were captured in JCAM. We also reconciled a judgmental sample of inventory records in JCAM to supporting documentation to determine if the data was accurate and complied with applicable policy guidance. Lastly, we interviewed OCIO officials, privacy officials from OPCL, and IT staff from JMD, EOUSA and the USMS. The number of sampled information systems from each component, including their operational status at the time of our review, are as follows:

Total number of JMD information systems sampled: 17

- Operational systems: 11
- New systems in the initiation phase: 2
- Retired systems no longer in operation: 4

Total number of EOUSA information systems sampled: 9

- Operational systems: 6
- New systems in the initiation phase: 1
- Systems in development: 1
- Retired systems no longer in operation: 1

Total number of USMS information systems sampled: 16

- Operational systems: 14 (10 were selected for privacy data testing only)
- Systems in development: 1
- Retired systems no longer in operation: 1

### Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

## Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objective. We did not evaluate the internal controls of JMD, EOUSA, and the USMS to provide assurance on the internal control structures as a whole. JMD, EOUSA, and USMS management are responsible for the establishment and maintenance of internal controls in accordance with Office of Management and Budget Circular A-123. Because we do not express an opinion on JMD, EOUSA, and the USMS's internal control structure as a whole, we offer this statement solely for the information and use of JMD, EOUSA, and the USMS.[9]

We assessed the design, implementation, and operating effectiveness of these internal controls and identified deficiencies that we believe could affect the Department's ability to effectively manage its inventory of information systems. The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the objective of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

## Compliance with Laws and Regulations

In this audit we also tested, as appropriate given our audit objective and scope, selected records, procedures, and practices, to obtain reasonable assurance that JMD, EOUSA, and the USMS's management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of our audit. Our audit included examining, on a test basis, the Department's compliance with the Federal Information Security Modernization Act and Section 208 of the E-Government Act of 2002 that could have a material effect on the Department's operations.

This testing included interviewing Departmental IT staff, analyzing JCAM data, assessing Department and component-level IT inventory policies, and examining IT inventory management practices. Nothing came to our attention that caused us to believe that the Department was not in compliance with the aforementioned laws and regulations.

## Sample-Based Testing

To accomplish our audit objective, we performed sample-based testing to verify the completeness and accuracy of JMD, EOUSA, and the USMS's information system inventory maintained in JCAM. In this effort, we employed a judgmental sampling design to obtain broad exposure to numerous facets of the areas we reviewed. This non-statistical sample design did not allow projection of the test results to the universe from which the samples were selected.

## Computer-Processed Data

During our audit, we obtained information from JCAM. We did not test the reliability of JCAM as a whole, therefore any findings identified involving information from that system was verified with documentation from other sources.

[9] This restriction is not intended to limit the distribution of this report, which is a matter of public record.

We assessed the reliability of the IT inventory data stored in JCAM by (1) verifying the existence of required inventory data and documents, (2) reconciling the inventory data entries to supporting documentation, and (3) interviewing auditee officials knowledgeable about the data. We determined that the data was sufficiently reliable for the purpose of drawing conclusions about the completeness and accuracy of the Department's inventory data.

# APPENDIX 2: JMD and OPCL's Response to the Draft Audit Report

**U.S. Department of Justice**

*Washington, DC 20530*

MEMORANDUM FOR JASON R. MALMSTROM
ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL

FROM: Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
Office of Privacy and Civil Liberties

Thomas Weikle
Assistant Director
Cybersecurity Services Staff

SUBJECT: Response for the Department of Justice Information System Inventory Management Audit

The Department of Justice (DOJ) Justice Management Division (JMD) and the Office of Privacy and Civil Liberties (OPCL) have reviewed the Office of the Inspector General Draft Audit Report for the DOJ Information System Inventory Management audit. JMD and OPCL concur with the findings and subsequent recommendations issued by the OIG.

In response, JMD and OPCL developed the actions outlined below to ensure they align with the recommendations identified and support the Department's efforts to enhance inventory accuracy, consolidate guidance, and further strengthen cybersecurity oversight.

OIG recommends JMD:

1. Establish clear data entry standards, including supporting document linkages, file naming conventions, and update schedules for the system inventory data stored in the Joint Cybersecurity Authorization and Management (JCAM) tool.

   Management Response

   JMD concurs with this recommendation. The audit identified inconsistent and outdated JCAM records due to the absence of detailed guidance specifying how information should be documented and maintained. To address these issues, JMD will develop a JCAM Data Entry Standards Guide establishing mandatory data-entry formats, proper document linkages, naming conventions, and update schedules.

2. Establish requirements to document justifications for special system categorizations in JCAM, such as Federal Information Security Modernization Act (FISMA) reportability, mission essential systems, critical infrastructure, and high value assets.

   Management Response

   JMD concurs with this recommendation. The audit identified systems lacking documentation to support key categorizations, including FISMA reportability. To address these gaps, JMD will implement a standardized categorization justification template aligned with Security and Privacy Assessment & Authorization Handbook (SPAA) criteria and establish JMD review checkpoints during system registration and annual updates.

3. Consolidate IT inventory recordkeeping guidance to ensure consistent management and maintenance of information system data across all components.

   Management Response

   JMD concurs with this recommendation. The audit found that IT inventory requirements are dispersed across multiple policy documents. To improve consistency and clarity, JMD will consolidate all recordkeeping requirements within the SPA&A, centralize the JCAM user guide in the Office of the Chief Information Officer document library, and coordinate with the JCAM team to routinely update training and onboarding materials.

4. Develop and implement a plan for performing regular inventory validations across all DOJ information systems.

   Management Response

   JMD concurs with this recommendation. The audit determined that DOJ lacks the process to validate non-FISMA reportable systems. To strengthen oversight, JMD will establish an annual Department-wide inventory validation process and incorporate Component best practices for more frequent system inventory validation.

OIG's recommendation that OPCL:

5. Evaluate the privacy workflow process and collaborate with components to streamline the IPA and PIA review, approval, and documentation processes to ensure timely completion of privacy assessments.

   Management Response

   OPCL concurs with this recommendation. Over the past year, OPCL has discussed improvements to and clarification of the privacy workflow processes with staff and DOJ components. OPCL plans to finalize these improvements and clarifications and roll them out to components. Within 90 days, OPCL plans to finalize privacy workflow

improvements and clarification. Within the next year, OPCL plans to roll out these improvements and clarifications to component privacy and information system security personnel, including related training.

If we may be of further assistance to you, please do not hesitate to contact us. Your staff may also contact Mike Terry or Brian Young at OPCL.

# APPENDIX 3: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

The OIG provided a draft of this audit report to the Justice Management Division (JMD) and the Office of Privacy and Civil Liberties (OPCL). JMD and OPCL's joint response is incorporated as Appendix 2 of this final report. In response to our draft audit report, JMD and OPCL concurred with our recommendations and discussed the actions they will implement in response to our findings. As a result, the audit report is resolved. The following provides the Office of the Inspector General's analysis of the response and summary of actions necessary to close the report.

**Recommendations for JMD:**

1. **Establish clear data entry standards, including supporting document linkages, file naming conventions, and update schedules for the system inventory data stored in the Joint Cybersecurity Authorization Management application (JCAM).**

   Resolved. JMD concurred with our recommendation. JMD stated in its response that it will develop a JCAM Data Entry Standards Guide establishing mandatory data-entry formats, proper document linkages, naming conventions, and update schedules.

   This recommendation can be closed when we receive the finalized JCAM Data Entry Standards Guide establishing mandatory JCAM data entry standards.

2. **Establish requirements to document justifications for special system categorizations in JCAM, such as Federal Information Security Modernization Act (FISMA) reportability, mission essential systems, critical infrastructure, and high value assets.**

   Resolved. JMD concurred with our recommendation. JMD stated in its response that it will implement a standardized categorization justification template aligned with DOJ Security Privacy Assessment and Authorization Handbook (SPAA) criteria and establish JMD review checkpoints during system registration and annual updates.

   This recommendation can be closed when we receive evidence that JMD has implemented a standardized system categorization justification template and established categorization review checkpoints.

3. **Consolidate IT inventory recordkeeping guidance to ensure consistent management and maintenance of information system data across all components.**

   Resolved. JMD concurred with our recommendation. JMD stated in its response that it will consolidate all recordkeeping requirements within the SPAA, centralize the JCAM user guide in the Office of the Chief Information Officer (OCIO) document library, and coordinate with the JCAM team to routinely update training and onboarding materials.

This recommendation can be closed when we receive evidence that JMD has consolidated all recordkeeping requirements within the SPAA, made available in the OCIO document library the JCAM Data Entry Standards Guide developed in Recommendation 1, and coordinated with the JCAM team to ensure consistent management and maintenance of information system data across all components.

4. **Develop and implement a plan for performing regular inventory validations across all DOJ information systems. The plan should consider existing best practices, including the United States Marshals Service (USMS) monthly validation process, to ensure JCAM records for each system are complete and accurate.**

   Resolved. JMD concurred with our recommendation. In its response, JMD stated that it will establish an annual Department-wide inventory validation process and incorporate DOJ component best practices for more frequent system inventory validation.

   This recommendation can be closed when we receive evidence that JMD has established an annual Department-wide inventory validation process that ensures all DOJ information systems are accurately and completely recorded in JCAM.

**Recommendations for OPCL:**

5. **Evaluate the privacy workflow process and collaborate with components to streamline the Initial Privacy Assessment (IPA) and Privacy Impact Assessment (PIA) review, approval, and documentation processes to ensure timely completion of privacy assessments.**

   Resolved. OPCL concurred with our recommendation. In its response, OPCL stated that it has worked with DOJ components to identify necessary improvements to, and clarifications of, the privacy workflow process. Within 90 days, OPCL plans to finalize those privacy workflow improvements and clarifications. OPCL also stated that, within the next year, it plans to roll out these improvements and clarifications to component privacy and information system security personnel, including related training.

   This recommendation can be closed when we receive evidence that OPCL has collaborated with DOJ components to identify and implement improvements to, and clarifications of, the privacy workflow process to ensure timely completion of privacy assessments.