Data Strategy for the U.S. Department of Justice

December 2022

U.S. Department of Justice
Office of the Chief Information Officer

Contents

Message from the Chief Data Officer

I am pleased to present this update to the U.S. Department of Justice (DOJ) Data Strategy. This Strategy outlines DOJ's ongoing approach to manage, use, and share data, as well as advance our data communities.

We continue to prioritize our data as a strategic asset around which we build systems and services. The long-term objective of this Strategy remains to optimize the value of DOJ data assets for use in our missions. The Strategy also aims to encourage public usage and engagement through open data. Using an incremental and collaborative process, we mature our data capabilities in a way that minimizes impacts to our stakeholders.

Our Strategy shapes support for DOJ missions and builds our capacity for data-driven decision-making. To leverage rapid advances in technology, DOJ must continue to establish and refine our enterprise-wide approaches for data management; information sharing; Identity, Credential, and Access Management (ICAM); and sustainable data culture. Through this Strategy, we build upon a solid foundation of success.

Sincerely,

Melinda Rogers
Deputy Assistant Attorney General
Chief Data Officer
Chief Information Officer
U.S. Department of Justice

Introduction

"Continue to strengthen Federal data management practices and infrastructure and enhance data science skills to promote efficient, equitable, and appropriate use of Federal data by Federal agencies and the public."
— President's Management Agenda, 2021

Timely access to reliable and useful information is critical to the successful execution of the U.S. Department of Justice (Department, or DOJ) mission. Consistent with the President's Management Agenda, the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), the Geospatial Data Act of 2018, and the Federal Data Strategy, and in accordance with all applicable statutory and regulatory requirements, the DOJ Data Strategy continues to build enterprise capabilities for data management, information sharing, controlled access, and a modern and relevant data workforce. The long-term objective is to optimize the impact of data and related information technology investments on the mission, the people serving the mission, and the public. The short-term objective is to do this in a manner that minimizes the burden and disruption to DOJ components and mission operators.

This Strategy recognizes that DOJ entrusts the management of data to the Chief Data Officer (CDO), mission holders, data stewards, system owners, records officers and managers, DOJ component CDOs, and DOJ component Chief Information Officers (CIOs). They hold the responsibility to ensure appropriate use, access, and stewardship of their data. Accordingly, nothing in this Strategy requires or expects sharing of information or other action that contravenes existing DOJ component legal requirements or business/mission considerations. The DOJ CDO, however, also shares accountability for the effective development and execution of data architectures, policies, practices, and procedures and, in coordination with the Evaluation Officer and the Statistical Official, for building capacity for evidence-based policymaking and data-driven decision making. Through this Strategy, and in conjunction with the DOJ Geospatial Data Strategy and Artificial Intelligence (AI) Strategy, DOJ promotes transparency, accountability, and alignment across mission operations and enterprise capabilities. This Strategy encourages the development of data communities to support comparable mission operations with similar but unique data and policy requirements and build DOJ-wide capacity, to the maximum extent possible consistent with pre-existing DOJ component data stewardship responsibilities and business/mission considerations.

The purpose of the DOJ Data Strategy is to promote awareness, use, and reuse of DOJ data assets to the maximum extent possible, without superseding the DOJ component responsibility in determining what information must be shared or with whom. This Strategy is a roadmap for developing and maturing enterprise data capabilities. Any DOJ component-level data strategy must align with this Strategy, thereby affirming DOJ component responsibility to actively manage, appropriately share, and make decisions about their data based on business cases and legal requirements. DOJ component CDOs and CIOs continue to work with their data stewards, system owners, and records managers to identify opportunities across their respective data community (e.g., law enforcement, legal, etc.) to help determine if what they are doing might be useful to another member of the community, or inform an enterprise or community standard or policy.

By building upon existing DOJ best practices, this Strategy advances an enterprise framework that prioritizes basic data capabilities before advanced ones. The Strategy promotes incremental and collaborative progress over high-risk, or so-called “big-bang” solutions, recognizing that a one-size approach does not fit all and that the DOJ and mission operations are nuanced and dynamic.

This document advances the existing foundation for DOJ data assets and data management capabilities in order to maximize their value to the mission through emerging technologies and innovations, such as advanced analytics, machine learning, and AI. Fully executed, this Strategy enables DOJ to streamline mission support and provides a programmatic approach to managing, sharing, and advancing data capabilities across its community.

Goals

The DOJ Data Strategy outlines the following four goals that provide a sustainable data culture and maximize the full value of our data assets:

Goal One:
Enterprise Data Management

Goal Two:
Enterprise Information Sharing Capability

Goal Three:
Enterprise Identity, Credential, and Access Management

Goal Four:
Enterprise Data Workforce

For each goal, the Strategy outlines specific actions, desired outcomes, and responsibilities for implementation at both the DOJ component and enterprise levels. Only through collaboration within and across DOJ components will success be achieved.

Goal One: Enterprise Data Management

Develop and execute architectures, policies, practices, and procedures that properly manage the full data lifecycle needs of DOJ.

Action: Establish and align data policies; specify roles and responsibilities for data retention, privacy, security, and confidentiality; encourage collaboration through data communities; monitor policy and standards for compliance and effectiveness using key performance indicators (KPIs); and review and incorporate unique mission requirements.

Outcome: Mission operators and stakeholders realize improved quality and access to mission data for decision-making. Data communities identify analytics initiatives that address agency and mission challenges. Enterprise data governance provides accountability and ensures investments are incorporating data policy and standards, including records management policies, standards, and responsibilities, throughout all phases of the information lifecycle. DOJ data management standards and practices are accessible to all of DOJ components.

Enterprise Responsibilities: The DOJ Data Governance Board promotes effective and efficient use of data, aligns architectures with emerging technologies, and advances the privacy (including personally identifiable information, or PII), security, confidentiality, and stewardship interests of data throughout DOJ. In alignment with statutory, policy, and regulatory requirements, the DOJ Data Governance Board brings together the critical data stakeholders across the enterprise to:

- Maintain DOJ Data Governance Board materials on the public website;
- Review the DOJ Data Strategy, Geospatial Data Strategy, and Artificial Intelligence (AI) Strategy to determine if any updates are needed based on the specified requirements and authorities of the Evidence Act, Geospatial Data Act, Federal Data Strategy;
- Maintain CDO and data responsibilities in DOJ policy; determine if any policy updates are needed based on Data Strategy deliverables or federal requirements;
- Maintain a standardized set of terminology for data management; maintain a foundational data management lifecycle; and maintain the types and scope of data within DOJ;
- Maintain data management roles and responsibilities; maintain and support data communities and data stewards;
- Maintain DOJ-wide data standards and best practices;
- Create guidelines for assessing the risk for the purpose of populating the DOJ data catalog;
- Review inventory of data assets to ensure data stewards are appropriately populating the DOJ data catalog;

- Provide data management templates for use by DOJ components and data stewards;
- Continue to assess the impact of DOJ policy, procedures, and guidance on how DOJ components use data to accomplish their mission;
- Develop a process plan for responding to public comments and requests regarding public DOJ datasets; and develop a process plan for analyzing open data usage and user types;
- Review, prioritize, and incorporate unique DOJ component data management requirements as submitted;
- Measure a core set of metrics for data management and frequency of reporting;
- Continue to assess and report on DOJ data assets and data capability, leveraging existing maturity models;
- Support identification and refinement of Priority Agency Questions;
- Annually update the strategic information resources management plan; and
- Publish an annual CDO report to Congress.

DOJ OCIO Responsibilities:

- Maintain the charter of the DOJ Data Governance Board;
- Report membership of DOJ Data Governance Board to U.S. Office of Management and Budget (OMB);
- Identify, assess, and coordinate with the DOJ Data Governance Board on new statutory, regulatory, and policy requirements impacting management of DOJ data;
- Maintain a DOJ-wide data catalog that contains agreed-upon metadata fields;
- Maintain data management standards and practices in a central reference material;
- Integrate data management plans into the Cybersecurity Assessment and Management (CSAM) system as required controls;
- Review and approve DOJ component data strategies;
- Publish DOJ datasets to Data.gov;
- Perform gap analysis on Open Data Plan to address requirements in OMB Evidence Act Phase 2 guidance;
- Maintain a process to evaluate and improve the quality of DOJ open government data assets; and
- Incorporate revisions to DOJ Data Strategy and publish.

DOJ Component Responsibilities: DOJ component CDOs and data stewards are responsible for executing enterprise data management practices. DOJ components must understand their information, ensure appropriate controls, access, and documentation, and participate in departmental working groups. DOJ component CDOs work with data stewards and mission operators to:

- Ensure DOJ component policies, practices, and procedures that support mission operations;
- Align DOJ component investments with enterprise data management practices;
- Determine if a DOJ component-level data strategy is required, and submit any developed strategy to the DOJ CDO for approval;
- Submit data management plans as part of the Authorization to Operate (ATO) package for all Federal Information Security Management Act of 2002 (FISMA) systems;
- Add and update datasets in the DOJ data catalog;
- Perform risk assessments on individual data assets and submit only appropriate items for publishing within the DOJ data catalog;
- Identify, document, and report unique data requirements to the DOJ Data Governance Board;
- Identify data needs to answer Priority Agency Questions; and
- Continue to assess and report data capabilities.

Goal Two: Enterprise Information Sharing Capability

Promote DOJ-wide capabilities for the appropriate and efficient sharing of information.

Action: Maintain a DOJ data exchange framework (also known as an information exchange framework) for DOJ components to document, control, and standardize how information is exchanged; establish and align data exchange policies; specify roles and responsibilities; inventory data exchanges within the DOJ data catalog; and review and incorporate unique mission requirements.

Outcome: Mission operators and stakeholders leverage the DOJ data catalog and data exchange framework enabling appropriate use of information and efficient and uniform information sharing. The DOJ data exchange framework promotes accountability, transparency, and collaboration across DOJ. DOJ information sharing standards and practices are available to all across DOJ.

Enterprise Responsibilities: The DOJ Data Governance Board is responsible for the development, documentation, and the DOJ-wide use of standards-based data exchanges. In alignment with statutory, policy, and regulatory requirements, the DOJ Data Governance Board brings together the critical data exchange stakeholders from across DOJ to:

- Establish understanding of the types and scope of data exchanges; maintain related roles and responsibilities for data exchanges; and identify data exchange communities;
- Develop principles, requirements, standards, and guidance for information sharing, emphasizing the use of application programming interface (API) technology;
- Create guidelines for appropriately inventorying how data is exchanged for the purpose of populating the DOJ data catalog;
- Create guidelines for assessing the risk for how data is exchanged for the purpose of populating the DOJ data catalog;
- Ensure data stewards are appropriately populating the DOJ data catalog with data exchanges;
- Develop a method to measure reuse of information in data exchanges;
- Develop recommendations for optimizing use of data exchanges; and
- Review, prioritize, and incorporate unique data exchange requirements as submitted.

DOJ OCIO Responsibilities:

- Develop a DOJ data catalog that includes an inventory of data exchanges inclusive of APIs, methods, who is responsible for data, and who has access; and
- Identify and publish data exchange standards in a central reference material.

DOJ Component Responsibilities: DOJ component CDOs and data stewards are responsible for executing appropriate data exchanges for their operations. DOJ components must understand their data exchanges, ensure appropriate controls, access and documentation, and participate in departmental working groups. DOJ component CDOs work with data stewards and mission operators to:

- Inventory and document external data exchanges within the data management plan for each FISMA system;
- Populate and maintain the DOJ data catalog with data exchanges to the extent consistent with existing legal and business/mission data stewardship requirements and obligations;
- Identify, document, and report unique data exchange standards to the DOJ Data Governance Board; and
- Ensure data exchanges comply with requirements and guidance.

Goal Three: Enterprise Identity, Credential, and Access Management

Provide secure, appropriate, timely, cost-effective, and efficient access to mission-critical information.

Action: Enable DOJ-wide identity assurance and accredited access across all DOJ enclaves through centralized credentialing and standard management to all DOJ FISMA systems and data. Document DOJ enterprise identity, credential, and access management (ICAM) standards and practices.

Outcome: Authorized users have secure, appropriate, timely, cost-effective, and efficient access to mission-critical information. All DOJ FISMA systems use a common ICAM capability. ICAM provides simplified sign-on, support for mobility, and inherent agility that keeps up with evolving mission and security requirements.

Enterprise Responsibilities: The DOJ CIO Council Cybersecurity Committee is responsible for DOJ-wide implementation of enterprise ICAM. To enable enterprise ICAM capabilities the DOJ CIO Council Cybersecurity Committee coordinates with the Data Governance Board to bring together the critical stakeholders across DOJ to:

- Continue to assess how ICAM policy, procedures, and guidance impact DOJ component missions; and
- Create ICAM metrics at the application level to validate the implementation of ICAM policy at the DOJ component-level.

DOJ OCIO Responsibilities:

- Maintain a comprehensive set of enterprise ICAM services to enhance integration, streamline related processes, and improve security posture across the enterprise;
- Maintain DOJ Identity and Access Management (IamDOJ) as the official system of record for all DOJ identities; uniquely represent each person by an Enterprise Digital Identity (EDI); and enable governance and reporting on identity attributes, permissions, and their associated system accounts at all levels of the enterprise;
- Continue to implement an enterprise privileged access management tool for DOJ components to manage privileged user credentials, enabling streamlined account management processes, policies enforcement, and monitored use of privileged accounts across the enterprise;
- Report DOJ component progress against ICAM implementation metrics;
- Maintain ICAM standards in a central reference material; and
- Review unique DOJ component ICAM requirements and architecture.

DOJ Component Responsibilities: DOJ component CIOs are responsible for executing DOJ ICAM for their operations. DOJ components must understand their user and data access requirements, ensure appropriate controls, access and documentation, and participate in DOJ ICAM working groups. DOJ component CIOs work with data stewards and mission operators to:

- Integrate DOJ component directory or identity systems with IamDOJ;
- Implement Personal Identity Verification (PIV) for physical access to controlled facilities and logical access to controlled information systems;
- Use enterprise privileged access management tool for privileged user access to all DOJ core infrastructure systems (i.e., servers, mainframes, network devices, etc.);
- Update ICAM metrics at the application level; and
- Report unique requirements and ICAM architecture to the DOJ Chief Information Security Officer (CISO).

Goal Four: Enterprise Data Workforce

Build a sustainable data culture in a modern information technology (IT) workforce.

Action: Update position descriptions; prioritize workforce training efforts in data literacy; and build the organizational capacity to share workforce, culture, training; and skill set knowledge and insight across DOJ components.

Outcome: Mature organizational capabilities to attract and retain top data and IT personnel. Leadership promotes and fosters continuous learning. Career paths promote the development of data governance, usage, and analytics skills and credentials. DOJ components achieve excellence in core mission and foundational capabilities.

Enterprise Responsibilities: The Data Governance Board ensures roles and responsibilities for the enterprise data workforce are defined and harmonized across DOJ components and encourages a data-driven culture that prioritizes data use and data stewardship. The Data Governance Board brings together the critical mission and technology stakeholders from across DOJ to:

- Support the data skills required by mission operations;
- Share common position descriptions, definitions, and continuous learning methods;
- Assess and measure DOJ data workforce maturity;
- Compare current workforce data skills against needs; and
- Develop a plan to close gaps in workforce data skills and literacy.

DOJ OCIO Responsibilities:

- Develop an enterprise data workforce portal to share definitions, methods, and models; and
- Publish and keep current information supporting the development of a modern IT workforce.

DOJ Component Responsibilities: DOJ component CDOs and data stewards work with mission operators to:

- Actively manage their data workforce to meet current and emerging business requirements;
- Develop and deploy foundational capabilities consistent with enterprise guidance;
- Develop and implement capabilities specific to DOJ component missions, shifting from low-value to high-value work as much as possible;

- Develop and execute technical capabilities, including in-use and emerging technologies, specific to DOJ component missions;
- Assess and measure DOJ component data workforce maturity based on DOJ guidelines;
- Update data and IT-related position descriptions to be current and relevant; and
- Develop and implement a method to onboard resources to address acute requirements.

View the DOJ Geospatial Data Strategy and Artificial Intelligence Strategy on Justice.gov.

Appendix: Acronyms

AI	**Artificial Intelligence**
API	**Application Programming Interface**
ATO	**Authorization to Operate**
CDO	**Chief Data Officer**
CIO	**Chief Information Officer**
CISO	**Chief Information Security Officer**
CSAM	**Cybersecurity Assessment and Management**
DOJ	**U.S. Department of Justice**
EDI	**Enterprise Digital Identity**
FISMA	**Federal Information Security Modernization Act of 2014**
IamDOJ	**DOJ Identity and Access Management System**
IT	**Information Technology**
ICAM	**Identity, Credential, and Access Management**
KPI	**Key Performance Indicator**
OMB	**U.S. Office of Management and Budget**
PII	**Personally Identifiable Information**
PIV	**Personal Identity Verification**