Data Strategy for the U.S. Department of Justice

February 2019

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

Contents

Message from the CIO 3

Introduction 4

Goals 5

Goal One: Enterprise Data Management 6

Goal Two: Enterprise Information Sharing Capability....................8

Goal Three: Enterprise Identity, Credential, and Access Management 10

Goal Four: Enterprise Data Workforce 12

Message from the CIO

I am pleased to present the U.S. Department of Justice's first Data Strategy. This Strategy is a foundational framework that will enable the Department to build a standardized, programmatic approach to manage and share data as well as advance our data communities.

Our data is a strategic asset, a core component around which we build systems and services. The long-term objective of the Strategy is to optimize the value of the Department's data assets for use in our missions. The goals outlined in our Strategy are the first steps in this journey. Through an incremental and collaborative process, we will evolve our data capabilities in a way that minimizes impacts to our stakeholders.

Our Data Strategy represents a transformative moment for the Department and the way in which we support our missions. It is clear that the only way to leverage rapid advances in technology is to ensure the Department has enterprise-wide approaches for data management; information sharing; Identity, Credential, and Access Management (ICAM); and building a sustainable data culture. Through the work we will accomplish under this Strategy, we will set the Department on a solid foundation for success.

Sincerely,

Joseph F. Klimavicz
Deputy Assistant Attorney General
Chief Information Officer
Department of Justice

Introduction

"The use of data is transforming society, business, and the economy."
— President's Management Agenda

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

This Policy recognizes that the Department entrusts the management of its data to the mission holders, system owners, records officers and managers, Component Chief Information Officers (CIOs), as well as the newly created Chief Data Officer. They hold the responsibility to ensure appropriate use, access, and stewardship of their data. Accordingly, nothing in this Policy requires or expects sharing of information or other action that contravenes a Component's existing legal requirements or business/mission considerations. The Department CIO, however, also shares accountability for the effective development and execution of architectures, policies, practices, and procedures. Through this Data Strategy, DOJ promotes transparency, accountability, and alignment across mission operations and enterprise capabilities. It encourages the development of data communities to support comparable mission operations with similar but unique data and policy requirements, to the maximum extent possible consistent with each Component's pre-existing data stewardship responsibilities and business/mission considerations.

The purpose of the DOJ Data Strategy is to promote visibility to the maximum extent possible through publication of a data assets inventory, also known as a "data catalog," without superseding the DOJ Component's responsibility in determining what information must be shared or with whom. The Strategy is a roadmap for developing and maturing enterprise capabilities. Any Component-level data strategy must align with this strategy, thereby affirming the Component's responsibility to actively manage, appropriately share, and make decisions about their data based on business cases and legal requirements. Component CIOs should 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 community member, 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. It promotes incremental and collaborative progress over status quo or high-risk, big-bang solutions. It recognizes that a one-size approach does not fit all and that the Department and mission operations are nuanced and dynamic.

This document lays the technical foundation to maximize the value of the Department's data assets as well as its enterprise data management capabilities in order to exploit emerging technologies and innovations such as artificial intelligence, machine learning, and advanced analytics. Fully executed, this strategy enables the Department to streamline mission support, provide a programmatic approach to managing, sharing, and advancing data intelligence capabilities across the DOJ community.

Goals

The DOJ Data Strategy outlines the following four goals that, when implemented, will help build 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 Component and enterprise levels. Only through collaboration within and across Components will the Department achieve success

Goal One: Enterprise Data Management

The development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of the Department.

Action: Establish and align data policies; specify roles and responsibilities for data retention, privacy, security, and confidentiality; monitor policy and standards for compliance and effectiveness; and review and incorporate unique mission requirements.

Outcome: Mission operators and stakeholders realize improved utility and access to mission data for decision-making. 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. The Technical Reference Architecture (TRA) documents the Department's data management standards and practices.

Enterprise responsibilities: The DOJ Chief Information Officer Council (CIOC) will establish a Data Committee to promote effective and efficient use of data, align architectures with emerging technologies, and advance the privacy (including personally identifiable information), security, confidentiality, and stewardship interests of data throughout the Department. In alignment with statutory, policy, and regulatory requirements, the Data Committee, in concert with the Governance Committee, shall bring together the critical data stakeholders from across the Department to:

- Define the types and scope of data within the Department; document data management roles and responsibilities; and establish data communities and data stewards;
- Establish department-wide data policies, standards, and best practices for documenting in the TRA;
- Create guidelines for assessing the risk and appropriately inventorying individual data assets for the purpose of populating the Department's data catalog;
- Review inventory of data assets to ensure data stewards are appropriately populating the Department's data catalog;
- Develop data management plan templates for use by Components and data stewards;
- Assess the impact of Department policy, procedures, and guidance on how Components use data to accomplish their mission;
- Develop a process plan for responding to public comments and requests regarding public Department datasets;

- Review, prioritize, and incorporate unique requirements as submitted;
- Define a core set of metrics for data management and frequency of reporting; and
- Assess and report on the Department's data assets and data capability, leveraging existing models (e.g. the Federal Data Maturity Model).

DOJ OCIO shall:

- Identify, assess, and coordinate with the Data Committee on new statutory, regulatory, and policy requirements impacting management of the Department's data;
- Develop and maintain a department-wide data catalog containing fields for a metadata index containing agreed-upon metadata fields;
- Document standards and practices in the TRA;
- Integrate data management plans into the Cyber Security Accreditation Management (CSAM) system as required controls; and
- Review and approve Component data strategies.

DOJ Component responsibilities: DOJ Component CIOs 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 CIOs shall work with data stewards and mission operators to:

- Ensure Component policies, practices, and procedures support mission operations;
- Align Department's data management practices with Component investments;
- Determine if a Component-level data strategy is required, and submit any developed strategy to the Department CIO for approval;
- Submit data management plans as part of the Authorization to Operate package for all Federal Information Security Management Act (FISMA) systems;
- Perform risk assessments on individual data assets and submit only appropriate items for publishing within the Department's data catalog;
- Identify, document, and report unique data requirements to the CIOC Data and Governance Committees; and
- Assess and report capabilities.

Goal Two: Enterprise Information Sharing Capability

Department-wide capability to encourage the appropriate sharing of information.

Action: Develop 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 exchange policies; specify roles and responsibilities; inventory data exchanges within the Department's data catalog; 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 Department's data exchange framework promotes department-wide accountability. The TRA documents the DOJ information sharing standards and practices.

Enterprise responsibilities: The newly established DOJ CIOC Data Committee is responsible for the development, documentation, and the Department-wide use of standards-based data exchanges. In alignment with statutory, policy, and regulatory requirements, the Data Committee, in concert with the Governance Committee, shall bring together the critical data exchange stakeholders from across DOJ to:

- Define the types and scope of data exchanges; document related roles and responsibilities; and identify exchange communities;
- Develop principles, requirements, standards, and guidance for information sharing, emphasizing the use of application programming interface (API) technology, and document them in the TRA;
- Create guidelines for assessing the risk and appropriately inventorying how data is exchanged for the purpose of populating the Department's data catalog;
- Ensure data stewards are appropriately populating the Department's data catalog with data exchanges;
- Develop a method to measure exchange reuse and make recommendations for optimization; and
- Review, prioritize, and incorporate unique requirements

DOJ OCIO shall:

- 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 to it; and
- Identify and publish data exchange standards in the TRA.

DOJ Component responsibilities: DOJ Component CIOs 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 CIOs shall work with data stewards and mission operators to:

- Within the data management plan for each FISMA system, inventory and document external data exchanges;
- Populate and maintain the Department's 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 CIOC Data and Governance Committees; and
- Ensure data exchanges comply with requirements and guidance in the TRA.

Goal Three: Enterprise Identity, Credential, and Access Management

Enterprise capability to provide secure, appropriate, timely, cost-effective, and efficient access to mission-critical information.

Action: Enable Department-wide identity assurance and accredited access across all DOJ enclaves through centralized credentialing and standard management to all DOJ FISMA systems and data. The TRA documents DOJ's 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 CIOC Cybersecurity Committee is responsible for the department-wide implementation of enterprise ICAM. To enable enterprise ICAM capabilities the Cybersecurity Committee shall bring together the critical stakeholders from across the Department to:

- Assess how ICAM policy, procedures, and guidance impact the Component's mission; and
- Create ICAM metrics at the application level to validate the implementation of ICAM policy at the DOJ Component-level.

DOJ OCIO shall:

- Establish a comprehensive set of enterprise ICAM services to enhance integration, streamline related processes, and improve security posture across the enterprise;
- Implement DOJ Identity and Access Management (IamDOJ) as the official system of record for all DOJ identities; within IamDOJ, uniquely represent each person by an Enterprise Digital Identity (EDI); enable governance and reporting on identity attributes, permissions, and their associated system accounts at all levels of the enterprise;
- Implement Justice Privileged Access Manager (JPAM), an enterprise tool for Components to manage privileged user credentials, enabling streamlined account management processes, policies enforcement, and monitored use of privileged accounts across the enterprise;
- Report progress against ICAM implementation metrics;
- Publish ICAM standards in the TRA; and
- Review unique requirements and approve or reject exceptions.

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

- Integrate DOJ Component directory or identity systems with IamDOJ;
- Implement Personal Identity Verification (PIV) and Personal Identity Verification Interoperability (PIV-I) for physical access to controlled facilities and logical access to controlled information systems;
- Use JPAM 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 seek approval for exceptions from the DOJ Chief Information Security Officer (CISO).

Goal Four: Enterprise Data Workforce

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

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

Outcome: Develop and mature organizational capabilities to attract and retain top data and IT talent; leadership promotes and fosters continuous learning; career paths promote the development of records and information management skills and credentials; DOJ Components achieve excellence in core mission and foundational capabilities.

Enterprise responsibilities: The newly established DOJ CIOC Data Committee and the Governance Committee shall ensure roles and responsibilities for the enterprise data workforce are defined and harmonized across DOJ Components and encourage a data culture that prioritizes data use and data stewardship. The Data and Governance Committees shall bring together the critical mission and technology stakeholders from across the Department to:

- Identify the data skills required by mission operations;
- Share common position descriptions, definitions, and continuous learning methods; and
- Assess and measure the data workforce maturity of the Department.

DOJ OCIO shall:

- 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 CIOs shall 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's 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's missions;

- Assess and measure enterprise 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 Geospatial Data Strategy located on justice.gov.