NID 2800.149
NPD 2800.1
Effective Date: December 3, 2024
Expiration Date: December 3, 2025

Subject: NASA Data Governance, Roles, and Responsibilities

Responsible Office: Office of Chief Information Officer (OCIO)

Table of Contents

Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Roles and Responsibilities

1.1 The NASA Chief Data Officer (CDO) shall:
1.2 Administrator Staff Office Officials-In-Charge, Mission Directorate (MD) Officials-In-Charge, Mission Support Directorate (MSD) Officials-In-Charge, and Center Directors or their respective Deputy Associate Administrators or position of equal level shall:
1.3 Senior Data Officials shall:
1.4 Data Stewards shall:
1.5 Data Custodians shall:

Chapter 2. Federated Data Governance

2.1 Federated Data Governance
2.2 Data Governance Board (Agency level)
2.3 Data Management Boards (Organizational Level)
2.4 Additional Data Governance (Lower Levels)

Appendix A. Definitions

Appendix B. Acronyms

Change History

Chg #	Date	Description / Comments
1	10/15/2024	For Agency NID review

Preface

P.1 Purpose

a. This directive establishes NASA's approach for Data Governance and sets the associated Roles and Responsibilities needed to execute it. This NID provides additional guidelines and references to other data management policies to provide guidance for NASA employees to leverage and follow to execute effective data management.

b. This directive implements a federated data governance approach to empower organizations to tailor their data management practices to their needs in order to meet NASA mission objectives.

P.2 Applicability

a. This directive is applicable to NASA Headquarters and NASA Centers including Component Facilities and Technical and Service Support Centers. This directive applies to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, and other contractors only to the extent specified or referenced in applicable contracts.

b. This directive is applicable to other contractors, recipients of grants or cooperative agreements, or parties to other agreements only to the extent specified in contracts, grants or cooperative agreements, or other agreements.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice, and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. This document serves as the parent document to all NASA data management policies, guidelines, plans, or requirements which may be issued for a department, program, laboratory, office, mission, center, or other organizational unit. As the parent document, this directive provides broader guidance on the governance and management of all NASA data and internal data sharing. Appending to this Directive with domain or organizationally specific guidelines or standards is strongly encouraged. Space Act Agreements and external sharing outside the agency is not in scope of this directive.

e. Contracting Officers, as defined in Federal Acquisition Regulation 2.101, or Agreement Managers, as defined in NAII 1050.3, NASA Partnership Guide, shall ensure that: the requirements of this directive are included in all NASA contracts and other agreements pursuant to which NASA data is being processed or transmitted; IT devices are procured for a purpose that is not incidental to the contract, and/or IT devices are developed or used on a NASA network; and responsibility for the flow-down of the requirements of this directive to subcontractors and subcontractor adherence is maintained.

P.3 Authority

a. Federal Information Security Modernization Act (FISMA) 2014, 44 U.S.C. § 3551 et seq.

b. Paperwork Reduction Act of 1995, 44 U.S.C. § 3501, as amended.

c. Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435 (2019).

d. Federal Data Strategy 2020 Action Plan.

e. Federal Data Strategy 2021 Action Plan.

f. OMB Memorandum M-06-07, Designation of a Senior Agency Official for Geospatial Information, March 3, 2006.

g. OMB Memorandum M-13-13, Open Data Policy-Managing Information as an Asset, May 9, 2013.

h. OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022.

i. OMB Circular A-130 - Managing Information as a Strategic Resource.

j. NPD 1001.0, 2022 NASA Strategic Plan.

k. NPD 1210.7, NASA Evaluation Policy.

l. NPD 2800.1, Managing Information Technology.

m. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

n. NPR 7120.7, NASA Information Technology Program and Project Management Requirements.

o. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.

P.4 Applicable Documents and Forms

Document No.	Title
Pub. L. 114-185 5 USC, Section 552a	Privacy Act of 1974
Federal Register /Vol. 88, No. 38, 14 CFR Part 1212	Privacy Act - NASA Regulations
NPD 1000.3	The NASA Organization w/Change 116
NPD 1440.6	NASA Records Management
NPD 2810.1	NASA Information Security Policy
NPR 1382.1	NASA Privacy Procedural Requirements
NPR 1400.1	NASA Directives and Charters Procedural Requirements
NPR 1441.1	NASA Records Management Program Requirements
NPR 2810.1	Security of Information and Information Systems

NPR 2810.7	Controlled Unclassified Information
NASA-STD-2831	Metadata Standard for Data Discoverability
NASA Data Catalog Reference Architecture	NASA Data Catalog Reference Architecture
NASA Data Strategy	NASA Data Strategy
NASA IT Strategic Plan	NASA IT Strategic Plan
Guidance for implementing NSPM-33	National Science and Technology Council, Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development
OSTP Memo	OSTP, Ensuring Free, Immediate, and Equitable Access to Federally Funded Research

P.5 Measurement/Verification

a. Outcomes and performance measures related to the implementation of this policy are outlined in documents NPD 1001.0, NASA Data Strategy, and the NASA IT Strategic Plan. Results are reported through NASA's annual strategic review, OPEN Data Act Reporting, and reporting as directed by OMB.

P.6 Cancellation

a. N/A

Chapter 1. Roles and Responsibilities

1.1 The NASA Chief Data Officer (CDO) shall:

1.1.1 Serve as the principal data management official for the agency, overseeing agency-level data-related activities across all NASA mission areas.

1.1.2 Serve as an advisor to NASA's Administrator and senior leadership on matters pertaining to data, ensuring the alignment of data efforts with NASA's mission objectives.

1.1.3 Establish and chair (coordinate, convene, and recommend) the NASA Data Governance Board (DGB) and serve as the Agency Lead for Data Governance.

1.1.4 Represent NASA at C-level in Federal and inter-agency CDO forums.

1.1.5 Oversee strategic planning related to data management responsibilities, ensuring the integration of data-driven strategies to support the agency's research, operational, and administrative needs.

1.1.6 Promulgate agency level data policy, processes, artifacts, tools, standards, architectures, best practices, and other data guidance.

1.1.7 Review the development of data infrastructure to reduce barriers that inhibit data findability, access, interoperability, reuse, understandability, security, and trust (FAIRUST).

1.1.8 Ensure that data considerations (e.g., data rights clauses), are embedded within acquisition phases, developments, solution deployments, and operational maintenance/modernization cycles across the agency.

1.1.9 Collaborate with the Evaluation Officer and Statistical Officer in support of the NASA Evaluation Policy.

1.2 Administrator Staff Office Officials-In-Charge, Mission Directorate (MD) Officials-In-Charge, Mission Support Directorate (MSD) Officials-In-Charge, and Center Directors or their respective Deputy Associate Administrators or position of equal level shall:

1.2.1 Appoint a Senior Data Official to each Administrator Staff Office, MD, MSD, and Center, as defined in NPD 1000.3 to carry out the requirements set forth in this policy, herein referred to as a “Senior Data Official.”

1.2.2 Assure that mission enabling data sets within their organization have an active and accountable Data Steward(s), and Data Custodian(s) assigned.

1.3 Senior Data Officials shall:

1.3.1 Be accountable for and represent their domain or mission support function data needs.

1.3.2 Be a non-exclusive role, allowing them to hold additional data roles and responsibilities as needed.

1.3.3 Define and develop internal controls, including the creation of Data Management Plans, in coordination with Data Stewards to measure the effectiveness of their organization's data management practices.

1.3.4 Implement the processes and requirements defined in all applicable data standards, processes, and specifications established by the Chief Data Officer Federated Data Governance Framework (Section 2.1) including data governance artifacts.

1.3.5 Oversee the implementation of a Master and Reference data plan(s) appropriate to increase data management maturity, data quality, and data integration across data systems.

1.3.6 Be accountable for completing a data set inventory and ensuring their data sets are cataloged as directed by the CDO.

1.3.7 Be accountable for and establish data quality and data integrity controls for data assets within their domain or mission support function area.

1.3.8 Resolve definition conflicts for the business glossary and data dictionary created by Data Stewards, Section 1.4, for their domain or mission support function area.

1.3.9 Approve Data Sharing Agreements created by Data Stewards, Section 1.4, when acting as a Data Provider with Data Consumers to stipulate terms of use of the data to be exchanged.

1.3.10 Identify, apply, and review data handling rules applied to data sets within their domain or mission support function, ensuring consistent data management and guide use of data by Data Consumers outside their organization.

1.3.11 Ensure data access and sharing requests are approved in support of mission requirements for data sets where they are the Senior Data Official or a delegate which the Senior Data Official has defined.

1.3.12 Seek and satisfy new data needs through promotion of authorized sharing, when data is available, rather than initiating the creation or collection of new data.

1.3.13 Champion data governance within their domain or mission support function, ensuring data is defined so that it will be used in a consistent manner across the Agency.

1.3.14 Present data issues requiring adjudication to the Data Management Board (DMB) and the Data Governance Board (DGB) accordingly.

1.3.15 Participate in the Enterprise Data Working Group (EDWG).

1.3.16 Review and approve additional data awareness and training materials for their organization or domain area as necessary.

1.3.17 Appoint Data Stewards that will fulfill Data Steward responsibilities listed in Section 1.4, Data Stewards Shall.

1.3.18 Appoint Data Custodians who will fulfill Data Custodian responsibilities listed in Section 1.5, Data Custodians Shall.

1.3.19 Collaborate with the Data Stewards to promote and follow the NASA data policies for their domain or mission support function key data asset(s).

1.3.20 Provide guidance, make decisions, and offer leadership to Data Stewards and Data Custodians on data issues within their oversight.

1.3.21 Be NASA Civil Servants.

1.4 Data Stewards shall:

1.4.1 Be a non-exclusive role, allowing them to hold additional data roles and responsibilities as needed.

1.4.2 Facilitate, manage, and improve the quality of data assets in their organization, program or responsible data domain area (e.g., geospatial, human resources).

1.4.3 Be responsible for the day-to-day data management and data lifecycle.

1.4.4 Be responsible for ensuring data conforms to legal, regulatory, and operational standards.

1.4.5 Ensure requirements and settings defined in all available and applicable standards and specifications established by NASA are implemented for their domain or mission support function such as but not limited to, Metadata Standard for Data Discoverability NASA-STD-2831 and guidance documented in the NASA Data Catalog Reference Architecture.

1.4.6 Establish and implement a Master and Reference data plan appropriate to increase data management maturity, data quality, and data integration across data systems.

1.4.7 Follow standards, processes, and best practices for assuring the quality of metadata and data.

1.4.8 Be responsible for completing a data set inventory and ensuring their data sets are cataloged and tagged with standard descriptive metadata that enables improved discoverability.

1.4.9 Be able to define and describe all data they are assigned to and understand the data handling rules and processes that support it.

1.4.10 Develop, maintain, and approve a business glossary and data dictionary for all NASA data assets for which they are responsible.

1.4.11 Define how the data is to be used to enable consistent use of data for downstream Data Consumers.

1.4.12 Record the names of Senior Data Officials, Data Stewards, and Data Custodians in their data set inventory.

1.4.13 Establish procedures to appropriately classify data (e.g., Controlled Unclassified Information as required by NPR 2810.7) to meet data requirements at agency and federal level.

1.4.14 Establish Data Sharing Agreements when acting as a Data Provider.

1.4.15 Ensure data is accessible to authorized Data Consumers in accordance with Data Sharing Agreements.

1.4.16 Ensure Data Sharing Agreements stipulate the data handling rules and needs as defined by standards, policies, and their Senior Data Official's guidance when acting as a Data Provider.

1.4.17 Facilitate and monitor appropriate use of shared data sets by Data Consumers.

1.4.18 Support strategic activities including planning, policymaking, promoting data literacy, and ensure implementation and compliance of established organizational policies.

1.4.19 Support Senior Data Officials and work with Data Custodians to ensure required technical changes and controls are implemented and enforced.

1.4.20 Provide guidance and leadership for the Data Custodians (Section 1.5).

1.4.21 Identify and help resolve data issues, risks, and errors (escalating to Senior Data Official when required).

1.4.22 Participate in data-related working groups.

1.4.23 Participate in data awareness and training materials for their organization or domain area as necessary.

1.5 Data Custodians shall:

1.5.1 Be a non-exclusive role, allowing them to hold additional data roles and responsibilities as needed.

1.5.2 Be technical data experts of the systems, applications, and platforms that store and transfer data for which they are assigned.

1.5.3 Execute approved data quality and data integrity controls for data assets within their domain or mission support function area.

1.5.4 Identify and help resolve data issues, risks, and errors in the technical implementation of data solutions (escalating to Data Steward when required).

1.5.5 Monitor and manage application programming interfaces (APIs).

1.5.6 Administer access to data assets as granted by their Senior Data Official and maintain the lineage of their data as it is granted to Data Consumers.

1.5.7 Implement data handling rules applied to data sets they are accountable for to enable consistent data management and guide use of data by Data Consumers outside their organization.

1.5.8 Maintain a configuration document that represents data interfaces and exchanges between systems and data dictionaries for their domain or mission support function area.

1.5.9 Provide the infrastructure and support required for the delivery of quality data to Data Consumers.

1.5.10 Coordinate with Data Stewards to understand technical needs and implement technical changes.

1.5.11 Support Data Stewards to enable the definition and documentation of metadata and cataloging of data related products including nomenclature, schemas, definitions, etc.

1.5.12 Support Data Stewards in producing artifacts of data governance onboarding assuring the quality of artifacts required including accuracy, integrity, authenticity, usability, and reliability.

1.5.13 Participate in data-related working groups that govern the scope of data for which they are responsible.

1.5.14 Participate in data awareness and training materials for their organization or domain area as necessary.

1.5.15 When acting as a Data Consumer:

1.5.15.1 Be responsible for using data in compliance with data governance policies, data privacy laws, ethical guidelines, and any data sharing agreements made with the Data Provider.

1.5.15.2 Provide feedback on data quality and usability to Data Providers to enhance ongoing data governance and management efforts.

Chapter 2. Federated Data Governance

2.1 Federated Data Governance Framework

2.1.1 The Agency's Data Governance Framework is a federated management framework that offers latitude for mission directorates and centers to implement data governance that is optimized for their mission needs. It leverages a multi-tiered approach with responsibilities carried out at the agency level (enterprise), organizational level, and subordinate (tactical/program) levels as needed. The NASA data governance framework in this policy recognizes the Data Governance Board (DGB), which is part of the IT Strategy Board (ITSB), at the enterprise (NASA-wide) level and the Data Management Board (DMB) at the organizational level. This tiered framework is highly adaptable, and this policy grants the latitude for NASA organizations to implement data governance optimally to service their mission needs.

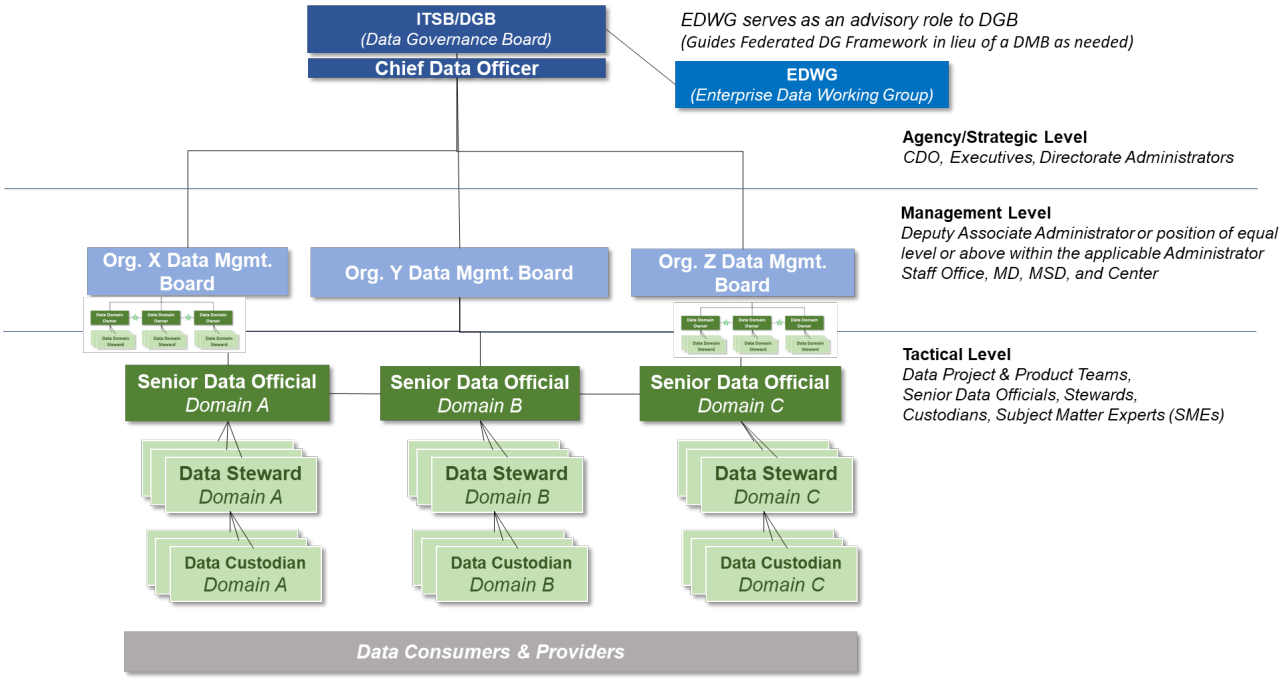

Figure 1. Federated Data Governance Framework

2.2 Data Governance Board (Agency level)

2.2.1 The Data Governance Board (DGB) is the agency-level, enterprise data governance function that makes decisions regarding data priorities, ownership, program, and projects that enable Data Governance at NASA. The DGB is part of the IT Strategy Board (ITSB), which serves as the Agency's decision-making board for IT strategy and data governance. The NASA Chief Data Officer is the decision authority of the Data Governance Board. The DGB:

2.2.1.1 Is responsible for setting NASA's agency level data mission objectives and data initiatives, and makes decisions on inter-agency data issues and disputes.

2.2.1.2 Serves as the final NASA approval authority for data management, data sharing, and data policy decisions that are elevated to the DGB.

2.2.1.3 Is the decision-making authority for the NASA Data Governance Framework and oversees the data governance process.

2.2.1.4 Approves and oversees NASA's implementation of the Federal Data Strategy Action Plan.

2.2.1.5 Directs and oversees the NASA Open Data Implementation Plan and its alignment with the Federal Chief Data Officer (CDO) Council Implementation Plan.

2.2.1.6 Oversees a recurring data set inventory to ensure an understanding of mission enabling data sets and the accuracy of the agency data catalogue.

2.2.1.7 Maintains an awareness of all Data Management Boards (DMBs) existing at NASA.

2.2.1.8 Adjudicates and resolves escalated issues, topics, or risks from the EDWG.

2.2.1.9 Issues directives, policies, and guidance for DMBs to follow.

2.3 Data Management Boards (Organizational Level)

2.3.1 Each Administrator Staff Office, MD, MSD, and Center defined in NPD 1000.3, may establish a DMB as mission need requires. Boards as defined in NPR 1400.1, requires a charter to operate and cite specific authority. The DMBs are the data governance function at the organizational level that exercises authority within their directorate or center setting data governance priorities and exercising authority over data management practices consistent with this policy. In lieu of a DMB, the EDWG can guide the Data Governance Federated Framework as needed.

2.3.2 The Deputy Associate Administrator or position of equal level or above within the applicable Administrator Staff Office, MD, MSD, and Center, or domain area may:

2.3.2.1 Create Data Management Boards to effectively govern data within their organization and manage data in support of mission and as required by this directive.

2.3.2.2 Be the DMB Decision Authority or delegate and authorize the Decision Authority position to an appointed Senior Data Official.

2.3.2.3 Serve as a principal in the DGB or be the senior advisor to their organization's DGB principal on organizational or program data topics. If they cannot attend, they must assign a delegate to attend the DGB meeting.

2.3.3 The DMBs:

2.3.3.1 Manage and make decisions that address the holistic data needs for their assigned domain area, including data standards, data integration, quality measures, and domain specific data management policies so long as they do not conflict with agency policy or data guidance.

2.3.3.2 Implement and maintain integrated data management and data governance across their organization or assigned data domain areas.

2.3.3.3 Ensure establishment of practices and guidelines for quality, security, and operational use of data assets, which adhere to established organizational processes practices, and guidelines.

2.3.3.4 Approve data guidance and Data Management Plans (DMPs) under the authority or oversight of their organization.

2.3.3.5 Follow legislation and organizational policies surrounding data assets including privacy, protected disclosures, communications, ethical considerations, records management.

2.3.3.6 Assist with data change management.

2.3.3.7 Ensure their domain data sets adhere to organizational or agency data governance practices, procedures, standards, and policies.

2.3.3.8 Coordinate with the DGB to develop and submit a DMB Charter and consult with the DGB as necessary on cross-cutting data management activities.

2.3.3.9 Inform the DGB on topics that have cross-cutting implications or benefit across NASA.

2.3.3.10 Escalate risks, issues, or unresolved decisions to the DGB as necessary.

2.4 Additional Data Governance (Lower Levels)

2.4.1 NASA organizations may implement additional governance that does not conflict with higher-level guidance as necessary to support the full scope of data management topics within their organization. If that should become necessary, those additional data governance functions should report to their organization's Data Management Board. Each organization defined in NPD 1000.3 may further define, delegate, and authorize any number of Senior Data Officials, Data Stewards, Data Custodians, and other data related boards or working groups as necessary to support their organizational data management needs.

Appendix A. Definitions

A.1 Definitions Table

Term	Definition
Accessible Data	Data accessibility is the degree to which people in an organization can use data per data provisioning controls. For data to be available, a user should only need to submit standard access requests implemented through standard technical services.
API	An application programming interface (API) is a predefined protocol for reading and/or writing data using a filesystem, a database, or across a network. Common types of data APIs include OBDC and SQL for databases and REST APIs for the web.
Artifact	An artifact is one of many kinds of tangible by-products produced during the process of data management programs - such as data dictionary and data glossary entries into software, and data lifecycle documentation collected during the Onboarding Process. Some development artifacts (e.g. conceptual and logical data models, data lineage) help document the interconnection, design, and flow of data and how it changes from one source to another. Other artifacts are concerned with the process of development itself—such as the on-boarding checklist, code review for data validity checking, project plans, etc.
Authoritative Data Source	A source of data or information that is recognized to be valid or trusted because its provenance is considered highly reliable or accurate. An authoritative source may be the functional combination of multiple, separate data sources. During the lifecycle process, the authoritative source (or system of use in which it is housed) can evolve according to use. Subject Matter Experts validate that the data is authoritative, and data management assures that data from the authoritative source is provided to users, and that it is current.
Business Glossary	Documentation of an organization's business concepts and terminology, definitions, and the relationships between those terms.
Catalog	A curated collection of metadata about resources (e.g., data sets, data services in the context of a data catalog), usually arranged systematically.
Change Management	Activities to educate the organization and encourage behaviors that enable strategic uses of data. Helping an organization move through the cultural changes that are necessary to embed effective data management practices.

Data	Data is a collection of discrete or continuous values that convey information, describing the quantity, quality, fact, statistics, other basic units of meaning, or simply sequences of symbols that may be further interpreted formally.
Data Access	The ability of a human or Non-Person Entity (NPE) to perform one or more operations on data, typically via service endpoints and Application Programming Interfaces (APIs). These operations may include the ability for data to be searched, retrieved, read, created, updated, deleted, manipulated, and executed.
Data Asset	A collection of data elements or data sets that may be grouped together. (44 U.S. Code § 3502). Data Assets are maintained and secured as a shared, critical, inexhaustible, durable, and strategic resource with the expectation of future value and benefits. Examples of data assets include databases, documents, data returned as web content, application/system output files and records.
Data Architecture	Data Architecture defines the blueprint for managing data assets by aligning with organizational strategy to establish strategic data requirements and designs to meet these requirements.
Data Catalog	A collection of metadata (usually combined with data management and search tools) that helps data Consumers find the data that they need. The data catalog serves as an inventory of available data and provides information to evaluate the fitness of data for intended uses.
Data Consumer	Any entity (which can be an individual, department, or external organization) that is a user and receiver of data (e.g., on a screen, in a report, through a query, via a machine-to-machine interface) from a Data Provider for analysis, decision-making, reporting, or other purposes. Data Consumers uses the data for a specific purpose and can be affected by its quality.
Data Custodian	Data Custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules. Data Stewards are responsible for what is stored in a data field, while Data Custodians are responsible for the technical environment and database structure. Data Custodians may typically identify as Database Administrators, IT Managers, System Administrators, etc.
Data Dictionary	The dictionary describes data in business terms and includes other information needed to use the data (e.g., data types, details of structure, security restrictions). Often the content for the data dictionary comes directly from the logical data model. Plan for high quality Metadata by ensuring modelers

	take a disciplined approach to managing definitions as part of the modeling process.
Data Domain	A distinct, logically grouped collection of data elements that share a common context. Each data domain is defined by its unique set of attributes, relationships, and rules that govern its usage and management. These domains are organized to align with the agency's operational areas, ensuring efficient data governance, quality control, and accessibility. Examples of data domains might include 'Personnel Management', 'Financial Transactions', 'Operational Metrics', and so forth. The structuring into data domains facilitates targeted data analysis, policy development, and decision-making, while also streamlining compliance with relevant data protection regulations.
Data Governance	A discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, conformance, and enforcement), which together administer data and information assets to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives.
Data Governance Onboarding	Data Governance On-boarding is the process, artifacts and audit reports to ensure that newly acquired data adheres to organizational standards for quality, security, privacy, and compliance and can be placed into the authoritative Data Governance. This process typically includes documenting data assets, assessing data quality, implementing data management practices, and ensuring that data assets are properly prepared and understood within the governance framework. The goal of data governance onboarding is to facilitate effective data management practices and mitigate risks associated with the use and integration of new data resources.
Data Handling	Data handling is concerned with how to procure, store, manage, use, and dispose of data.
Data Integration	Data Integration and Interoperability involves getting data where it is needed, when it is needed, and in the form in which it is needed. Data integration activities follow a development lifecycle. They begin with planning and move through design, development, testing, and implementation. Once implemented, integrated systems must be managed, monitored, and enhanced.
Data Integrity	The degree to which data can be trusted due to its provenance, pedigree, lineage and conformance with all business rules/data handling rules regarding its relationship with other data. In the context of data movement, the degree to which

	data has verifiably not been changed unexpectedly by a person or entity.
Data Inventory	A comprehensive list of the agency's data assets cataloged by metadata such as detailed information on the nature, location, format, ownership of data assets held by the agency from data catalog above. The data catalog serves as an inventory of available data and provides information to evaluate the fitness of data for intended uses.
Data Lifecycle	A conceptualization of a cradle-to-grave value chain for data, which often includes phases such as plan and task, acquire and assess, process and transform, discover and access, analyze and exploit, and preserve or dispose.
Data Lineage	A description of data's pathway from its source to its current location and the alterations made to the data along that pathway, which should be represented as a reproducible ancestry of the data object. Lineage can include traceability between parent and children data objects.
Data Literacy	Data literacy is the ability to understand data and data practices sufficiently to meaningfully interpret data and effectively communicate that meaning.
Data Management	Data Management is the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles. Data management activities are wide-ranging. They include everything from the ability to make consistent decisions about how to get strategic value from data to the technical deployment and performance of databases. Thus data management requires both technical and non-technical (i.e., 'business') skills. Responsibility for managing data must be shared between business and information technology roles, and people in both areas must be able to collaborate to ensure an organization has high quality data that meets its strategic needs.
Data Management Board (DMB)	The DMBs are the data governance function at the organizational level with line authority within their directorate, center, or data domain setting data governance priorities and exercising authority over data management practices.
Data Management Plan (DMP)	A plan that documents how specific data will be collected, processed, used and curated in order to facilitate long-term data management decisions and actions. It typically includes topics such as: a) Description of the data to be collected/created; b) Authority under which the data is collected;

	c) Standards/methodologies for data collection and management; d) Ethics and Intellectual Property concerns or restrictions; e) Plans for data sharing and access; and, f) Strategy for long-term preservation of the data.
Data Object	An instance of data that is discrete and bounded with an intrinsic, immutable, and unique identity that can persist independently of a system or service. A data object is made up of one or more data elements. For example, a row within a relational database or an image within an image library.
Data Platform	A data platform is any data centric technologies on which others are built and operated to provide interoperability, simplify implementation, streamline deployment and promote maintenance of solutions. The platform resource consists of hardware and system software, usually implemented as a platform service.
Data Product	A data product is a logical unit that contains all components to process and store domain data for analytical or data-intensive use cases and makes them available to other teams via output ports. Data products connect to sources, such as operational systems or other data products and perform data transformation. Data products serve data sets in one or many output ports.
Data Provider	Any entity (which can be an individual, department, or external organization) that is an authoritative source that creates, collects, maintains, and distributes data to another entity. They ensure the quality, accuracy, timeliness, and completeness of the data they supply to Data Consumers and adhere to established data governance standards, policies, and procedures, including those related to data privacy, security, and metadata management. Data Providers set clear business rules and guidance for the use of their data to ensure it is used appropriately.
Data Quality	Data Quality includes the planning and implementation of quality management techniques to measure, assess, and improve the fitness of data for use within an organization.
Data Set	One or more data objects that share common properties and characteristics, and are managed as a unit, often structured in a tabular form comprising of rows and columns. Each row typically represents a single record or observation, and each column represents a specific variable or attribute of that record. Data sets can vary in size from small, simple collections to large, complex compilations of data.
Data Sharing Agreements	Prior to the development of interfaces or the provision of data electronically, develop a data sharing agreement or

	memorandum of understanding (MOU) which stipulates the responsibilities and acceptable use of data to be exchanged between a Data Provider and data consumer, arranged by the Data Steward, and approved by the Senior Data Official of the data in question. The data sharing agreements should specify anticipated use and access to the data, restrictions on use, as well as expected service levels, including required system up times and response times. These agreements are especially critical for regulated industries, or when personal or secure information is involved.
Data Standard	A technical specification that describes how data should be stored or exchanged for the consistent collection and interoperability of that data across different systems, sources, and users.
Data Stewards	Data Stewards are accountable for the governance and maintenance of data within their domain or mission support function across the data lifecycle. Data Stewards may typically identify as Business Analysts, Leading Data S, etc. For more specific responsibilities, see Data Stewards Roles within this NID.
Data Tag	Metadata applied, through tagging to a data asset to help describe characteristics about the data, such as privacy, security, provenance, source, or other information, and can be used to support automated processing. A “tag” is an assertion describing some aspect of a resource, pairing a semantic label with a value (e.g., a document may have a tag name of “Language” with a corresponding tag value of “English”). The tag values may be known a priori (e.g., controlled vocabulary) or not (e.g., folksonomies).
Data Tagging	The act of associating data tags as metadata to a data object by identifying, labeling, and describing its information. Typically, tagging supports user interpretation and automated processing.
Data Type	A primitive data type is one of the most fundamental principles for defining what type of information a piece of data is. Common data types are: boolean, integer, string, and date.
Discovery	The act of obtaining knowledge of the existence, but not necessarily the content, of information [data] collected.
Domain	A logical grouping of data that is usually related by business function or subject area. It encompasses all the data relevant to a particular area of interest within an organization. Data domains help in organizing and managing data by providing a clear structure that aligns with business needs and processes.

	This Organization facilitates better data governance, data quality management, and overall data management practices.
Findable	According to FAIR principles, metadata and data should be easy to find for both humans and computers. Machine-readable metadata are essential for automatic discovery of data sets and services.
Format	The format or "serialization format" is the syntax, encoding, and file format or media type for storing or transmitting your data. On the web, formats are associated with standardized media type identifiers, like application/JSON. Common data formats include JSON, CSV, and XML.
Interoperable	According to FAIR Principles, the data usually needs to be integrated with other data. In addition, the data need to interoperate with applications or workflows for analysis, storage, and processing.
Master Data	Core mission and business data entities used in traditional or analytical applications across an organization, and subjected to enterprise governance policies, along with their associated metadata, attributes, definitions, roles, connections, and taxonomies. Master data provides context for mission and business activity data in the form of common and abstract concepts related to activity transactions, along with consistent and uniform set of identifiers and extended attributes that describe the core entities.
Metadata	Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher, or responsible party, contact information, method of collection, and other descriptions. (44 U.S. Code §3502)
Reuse	According to FAIR Principles, metadata and data (i.e. data assets, data pipelines, data platforms services, and data interfaces) should be well-described so that they can be replicated and/or combined in different settings.
Schema	A schema is a segmented division of data. There are other terms which are synonymous with schema, such as collection.
Secure	Secure means that Consumers know that data is protected from unauthorized use and manipulation.
Senior Data Official	A Senior Data Official is the senior agency official who has approval authority for decisions about data within their domain or mission support function. Senior Data Official may also be referred to as a Chief Data Officer or Data Officer to their respective Mission, Center, or domain area but in context of NASA work, will be referred to as Senior Data Official.

Structured Data	Content that conforms to a specific, pre-defined schema or data model, or is tagged or otherwise arranged into database tables (rows and columns). Examples include data in relational databases, data in graph databases, call data records, financial transactions, and system audit logs.
Trustworthy	Trustworthy means that Consumers can be confident that data can be used for decision making.
Understandable	Understandable means that Consumers can find descriptors of data to recognize the content, context, and applicability.
Unstructured Data	Content that does not conform to a specific, pre-defined data model, or is not tagged or otherwise structured into database tables (rows and columns). Examples include documents, presentations, graphics, images, text, reports, videos, or sound recordings.

Appendix B. Acronyms

B.1 Acronym Table Definitions

Acronym	Definition
CDO	Chief Data Officer
CUI	Controlled Unclassified Identifiers
DGB	Data Governance Board
DMB	Data Management Board
DMP	Data Management Plan
FAIRUST	Findability, Accessibility, Interoperability, Reusability, Understandability, Security, and Trustworthy
FISMA	Federal Information Security Modernization Act
GC	General Counsel
IT	Information Technology
ITSB	Information Technology Strategy Board
MD	Mission Directorate
MSD	Mission Support Directorate
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSPM	National Security Presidential Memorandum
OCIO	Office of the Chief Information Officer
OIC	Official-In-Charge
OMB	Office of Management and Budget
OSTP	Office of Science and Technology
SME	Subject Matter Expert
STD	Standard