Department of Defense

Chief Data Officer

DoD Data Stewardship Guidebook

October 2021

Table of Contents

1 Introduction

The Department of Defense (DoD) Data Stewardship Guidebook amplifies and extends key concepts from the DoD Data Strategy – three essential capabilities and five guiding principles. The essential capabilities enable the DoD Data Strategy goals and therefore, are leveraged within data stewardship roles and responsibilities to ensure that data is managed effectively at all levels. They empower the workforce to manage and maximize the value of data and to make data-informed decisions in implementing effectual processes. The guiding principles are foundational to all data efforts and enable military advantage by ensuring accountability throughout the data lifecycle, by providing access and availability to the fullest extent possible, and by keeping appropriate data sharing and use at the forefront.

The three (of four) essential capabilities leveraged in this guidebook are:

- ***Governance*** which provides the principles, policies, processes, frameworks, tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition.
- ***Talent and Culture*** which addresses the need to increasingly empower the DoD workforce (Service Members, Civilians, and Contractors at every echelon) to work with data, make data-informed decisions, create evidence-based policies, and implement effectual processes.
- ***Standards*** which provides a family of standards that includes not only commonly recognized approaches for the management and utilization of data assets, but also proven and successful methods for representing and sharing data.

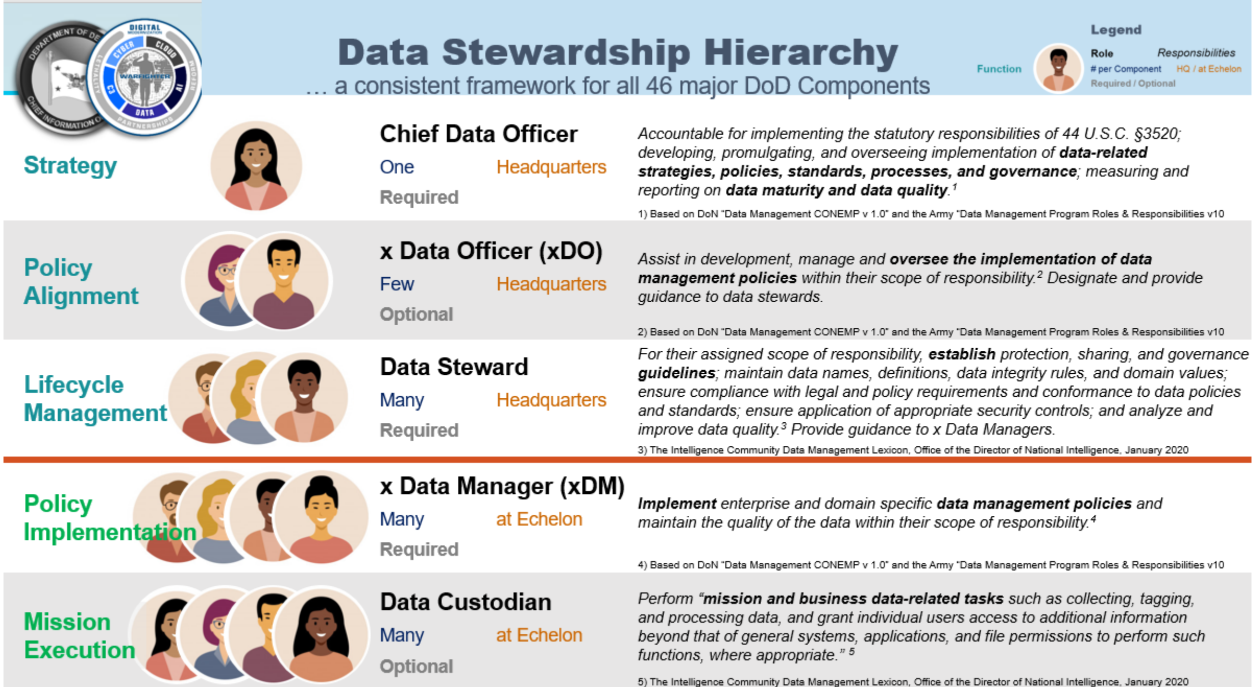
The five (of eight) guiding principles leveraged in this guidebook are:

- ***Data is a Strategic Asset*** – DoD data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage.
- ***Collective Data Stewardship*** – DoD must assign data stewards, data custodians, and a set of functional data managers to achieve accountability throughout the entire data lifecycle.
- ***Data Collection*** – DoD must enable electronic collection of data at the point of creation and maintain the pedigree of that data at all times.
- ***Enterprise-Wide Data Access and Availability*** – DoD data must be made available for use by all authorized individuals and non-person entities through appropriate mechanisms.
- ***Data Fit for Purpose*** – DoD must carefully consider any ethical concerns in data collection, sharing, use, rapid data integration as well as minimization of any sources of unintended bias.

The DoD Data Stewardship Guidebook identifies the roles and responsibilities necessary to govern and manage data on behalf of a DoD Component in support of the DoD Data Strategy. Roles within the guidebook should be recognized by leadership of DoD Components and empowered to perform data responsibilities. In doing so, data will become a strategic asset, a high value materiel that brings immediate and long lasting military advantage, furthering the three focus areas of the strategy: Joint All Domain Operations, Senior Leader Decision Support, and Business Analytics.

1.1 Data Stewardship Hierarchy

The Data Stewardship Hierarchy lays the foundation for data stewardship in the Department. The chart in Figure 1 summarizes how the key data stewardship roles and responsibilities interact and are executed. The guidebook includes detailed descriptions of these roles and responsibilities to ensure a common understanding and consistent implementation of data roles across DoD.



Data Stewardship Hierarchy

… a consistent framework for all 46 major DoD Components

Legend: Function — **Role** / # per Component / HQ / at Echelon / Required / Optional — *Responsibilities*

Function	Role	# per Component	HQ / at Echelon	Required / Optional	Responsibilities
Strategy	Chief Data Officer	One	Headquarters	Required	*Accountable for implementing the statutory responsibilities of 44 U.S.C. §3520; developing, promulgating, and overseeing implementation of* ***data-related strategies, policies, standards, processes, and governance****; measuring and reporting on* ***data maturity and data quality****.*[1]
Policy Alignment	x Data Officer (xDO)	Few	Headquarters	Optional	*Assist in development, manage and* ***oversee the implementation of data management policies*** *within their scope of responsibility.*[2] *Designate and provide guidance to data stewards.*
Lifecycle Management	Data Steward	Many	Headquarters	Required	*For their assigned scope of responsibility,* ***establish*** *protection, sharing, and governance* ***guidelines****; maintain data names, definitions, data integrity rules, and domain values; ensure compliance with legal and policy requirements and conformance to data policies and standards; ensure application of appropriate security controls; and analyze and improve data quality.*[3] *Provide guidance to x Data Managers.*
Policy Implementation	x Data Manager (xDM)	Many	at Echelon	Required	***Implement*** *enterprise and domain specific* ***data management policies*** *and maintain the quality of the data within their scope of responsibility.*[4]
Mission Execution	Data Custodian	Many	at Echelon	Optional	*Perform "****mission and business data-related tasks*** *such as collecting, tagging, and processing data, and grant individual users access to additional information beyond that of general systems, applications, and file permissions to perform such functions, where appropriate."* [5]

1) Based on DoN "Data Management CONEMP v 1.0" and the Army "Data Management Program Roles & Responsibilities v10

2) Based on DoN "Data Management CONEMP v 1.0" and the Army "Data Management Program Roles & Responsibilities v10

3) The Intelligence Community Data Management Lexicon, Office of the Director of National Intelligence, January 2020

4) Based on DoN "Data Management CONEMP v 1.0" and the Army "Data Management Program Roles & Responsibilities v10

5) The Intelligence Community Data Management Lexicon, Office of the Director of National Intelligence, January 2020

Figure 1: Data Stewardship Hierarchy

1.2 Data Stewardship Hierarchy Description

1. **46 Major DoD Components**
   The 46 major DoD Components are comprised of the Office of the Secretary of Defense (OSD), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General, the Military Departments (MILDEPS), and the Defense Agencies and DoD Field Activities (DAFAs).

2. **Functions**
   There are five functions (i.e., strategy, policy alignment, lifecycle management, policy implementation, and mission execution). Three are policy related and two are execution related.

   a. **Policy** – Functions above the red line are strategy, policy alignment, and lifecycle management. These functions set the foundation for the execution functions.

   b. **Execution** – Functions below the red line are policy implementation and mission execution.

3. **Number of Positions per DoD Component**
   The number of positions (one, few, many) is a guide, with the exception of the Chief Data Officer (CDO), where there can only be one. "Few" and "many" are relative to the number of major categories of data, and the size and responsibilities of the DoD Component. It is expected that the DoD Component exercise proper judgement in designating roles and responsibilities based on its mission(s) and the amount of data and data assets it manages.

4. **Required / Optional Roles**
   The establishment of specific roles or full time equivalents is deemed required or optional. Required roles and responsibilities are considered necessary for any DoD Component to function properly in accordance with the DoD Data Strategy essential capabilities of Governance and Talent and Culture. Optional roles are encouraged, but the responsibilities of these roles are essential to effective data management and are required to be carried out within the DoD Component regardless of position title. The need for optional roles is driven by DoD Component mission, manpower and size, and complexity of data assets.

5. **Headquarters / Echelon**
   The identification of the role being at headquarters or echelon is not necessarily a binary option. There are instances where it makes sense for the DoD Component to have certain roles at both. This attribute is intended to assist DoD Components in understanding where the roles most likely make sense and where those roles are likely to be performed.

6. **Responsibilities**
   The high level responsibility descriptions identify differences between the layers of the hierarchy. Greater detail is provided in Section 2 of this guidebook.

7. **"x" Qualifier**
   The "x" is used to provide flexibility in the naming of data officers. The DoD Component is given the flexibility to provide the appropriate term to describe how the DoD Component distributes the responsibility of the role. For example, if the DoD Component determines that it is best to use an existing or customized construct, such as Joint Capability Areas (JCAs), then they could have x Data Officers (xDOs) with titles like Force Management Data Officer, Health Readiness Data Officer, and Logistics Data Officer. Similarly, if a DoD Component chooses to use the Mission Area construct, they could have xDOs with titles like Warfighter Data Officer, Business Data Officer, Intelligence Data Officer, and Information Enterprise Data Officer. The xDO construct also supports organizational constructs where a MILDEP may have Installation Data Officers or a large Defense Agency may have xDOs based on their divisions/directorates.

   Likewise, for the x Data Manager (xDM) roles, the appropriate term should describe the responsibilities of the specific data manager such as their system or subsystem name (e.g., General Fund Enterprise Business System Data Manager) or their sub area of responsibility (e.g., Civilian Payroll Data Manager). These roles could also be data-functionally aligned with titles like Interoperability Data Manager, Data Quality Data Manager, Data Security Data Manager, and Metadata Data Manager. It is at the discretion of the DoD Component to identify the appropriate term for the roles that best address their organization.

   There is no restriction or requirement regarding the number of positions within a role that has an "x" qualifier. The DoD Component has the flexibility to assign the appropriate number of "x" qualifier roles based on their internal construct to meet mission.

2 Key Data Stewardship Roles and Responsibilities

This guidebook provides best practices to assist each DoD Component in implementing data stewardship within their organization. The goal is to promote consistent data stewardship across the Department. Data stewardship roles are not an additional layer of positions but rather existing positions in which people are performing identified data responsibilities. Each of the following roles and responsibilities are considered "best practices" and, as such, are essential to performing data stewardship in a manner that facilitates transformation of DoD into a data centric enterprise.

The Deputy Secretary of Defense memorandum, "Creating Data Advantage," directed DoD Components to coordinate their data activities by establishing appointed data leaders (e.g., CDOs). It is highly recommended that DoD Components implement all "required" roles and ensure coverage of responsibilities under "optional" roles unless justifications exist (e.g., business model does not require role, limited personnel). The responsibilities for all roles are essential in managing data throughout its lifecycle. DoD Components may designate existing, similar positions as dual roles to address the responsibilities identified in this guidebook; may determine if the role is a full or part time duty based on their mission and resources; or may assign roles/responsibilities according to type of staff (military, civilian, or contractor) in accordance with laws and regulations that restrict contractors from performing inherently governmental responsibilities. Recognizing that DoD Components are at different levels of data management maturity, there is no given timeline for implementation of these roles and responsibilities.

For the purposes of this document, data roles and responsibilities do not need to be exclusively tied to a traditional information system, as data and analytic platforms require data stewardship as well. Data stewardship does not address IT system hardware or software, but rather the data governance and data management activities related to databases, application programming interfaces (APIs), and other tools useful in managing data over its lifecycle.

The DoD CDO is responsible for issuing policy and guidance regarding the Department's data ecosystem (e.g., people, technology, and culture), data sharing, data architecture, data lifecycle management, and a data ready workforce. The Office of the DoD CDO collaborates with DoD Components on the development of policy to address areas where policy updates or guidance is needed. In circumstances where an issue cannot be resolved at the DoD Component level, the DoD CDO engages to find a suitable resolution. While 44 USC §3520 is a statutory requirement for the DoD CDO and the three MILDEP CDOs, these base requirements for data leadership should be guide the responsibilities of all appointed Component data leaders, including in CCMDs, DAFAs, and other sections of OSD.

2.1 DoD Component Chief Data Officer

Role Description
The DoD Component CDO is a designated senior official within each DoD Component responsible for the management of data as an asset. For the MILDEPS and DoD CDO that are subject to CDO requirements in U.S. Code (USC), they are accountable for implementing the appropriate statutory responsibilities of 44 USC §3520; for developing, promulgating, and overseeing implementation of data-related strategies, policies, standards, processes, and governance; and for measuring and reporting on data maturity and data quality.

Detailed Responsibilities

1. Implement appropriate functions of 44 USC §3520(c) in alignment with the DoD Data Strategy and other relevant strategies.
2. Address Federal Data Strategy (FDS) Action Plan (FDSAP) requirements when required or appropriate to improve data management within their DoD Component.
3. In cooperation with stakeholders, such as USD(A&S) and the acquisition community, pursue change across a broad spectrum of materiel and non-materiel solutions, and create policies around data management. These policies govern data management across the entire data lifecycle (from origination to disposition) and cover all types of data regardless of purpose or use.
4. Develop and oversee the DoD Component-level data management strategy and data management plan. The plan documents how specific data is collected/created, processed, used, maintained, and disposed in order to facilitate long-term data management decisions and actions. It should include 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
    f. Strategy for long-term preservation of the data.
    g. Metadata Management
    h. Interoperability and Data Exchange
    i. Security
    j. COOP/disaster recovery
    k. Data Governance and authority to govern (i.e., the plan should describe how the roles defined in this document are implemented.)
    l. Data Storage and Backup
    m. Data Archival/Disposal
5. Identify categories of data that should incorporate dynamic authorization and access to data.
6. Instantiate and oversee appropriate decision bodies, such as a Data Governance Board (DGB), to ensure establishment and enforcement of data governance.
7. In conjunction with other DoD Component stakeholders, including xDOs, create subdomains and appoint subject matter experts with detailed knowledge of specific data types unique to a subdomain. Define as many or as few subdomains as necessary.
8. Coordinate and involvement in acquisition decisions to ensure compliance with data policies.

2.2 x Data Officer

Role Description
xDOs develop, manage, and oversee the implementation of data management policies within their scope of responsibility. They designate and provide guidance to data stewards, and assist the DoD Component CDO and other senior officials with the development of DoD Component level data management policies.

Detailed Responsibilities

1. In coordination with the Component CDO, implement appropriate functions of 44 USC §3520(c) in alignment with the DoD Data Strategy and other relevant strategies.
2. Address FDSAP requirements when required or appropriate to improve data management within their scope of responsibility.
3. Be appointed by leaders within their area of responsibility in consultation with the DoD Component CDO. Report and coordinate with the CDO as organizationally appropriate.
4. In conjunction with the DoD Component CDO and other data stakeholders, create subdomains and appoint subject matter experts with detailed knowledge of specific data types unique to a subdomain. Define as many or as few subdomains as necessary.
5. Develop data policies, guidance, procedures, and standards related to a specific discipline and establish related training.
6. Drive change within organizational structure, information resources management policy, and technology solutions to improve decision support outcomes. Additionally, if appropriate, engage with secretariats, resource sponsors, and Budget Submitting Offices to recommend program improvements with respect to data governance and management.
7. If the DGB approves and promulgates data policies, procedures, standards, and specifications for implementation, implement and enforce DGB guidance for the DoD Component.
8. Protect and manage data as an asset and serve as senior advisor to the DoD Component head on all data matters within their scope of responsibility including:
    a. Developing and overseeing implementation of a data management plan
    b. Advising on funding allocation to implement the data management plan
    c. Coordinating enterprise data strategy, policies, standards, and enactment in fulfillment of their responsibilities
    d. Creating and sustaining a data-aware and data literate workforce
    e. Governing data, including its creation, use, analysis, protection, and destruction
    f. Coordinating with those developing architectures to facilitate the management and integration of DoD Component high-level data architecture and engineering products
    g. Approve and implement DoD Component data policies, standards, and specifications for data stewards within their respective domain.

9. Oversee data and the management of data within their area of responsibility:
    a. Coordinate integration of data across DoD Component applicable constructs (e.g., mission areas, information domains)
    b. Designate, assign, and task data stewards
    c. Define scope of data steward responsibility
    d. Report to DoD Component DGB.

2.3 Data Steward

Role Description

For their assigned scope of responsibility, data stewards establish protection, sharing, and governance guidelines; maintain data names, definitions, data integrity rules, and domain values; ensure compliance with legal and policy requirements, and conformance to data policies and standards; ensure application of appropriate security controls; and analyze and improve data quality. They provide guidance to xDMs.

Detailed Responsibilities

1. In coordination with the Component CDO, implement appropriate functions of 44 USC §3520(c).
2. Perform some or all of the following, depending on the DoD Component:
    a. Govern domain in accordance with DoD Component DGB Charter
    b. Attend and actively participate in enterprise data governance forums
    c. Assist with serving the interests and needs of their stakeholders
    d. Convey and support the positions and decisions of the DGB to their stakeholders
    e. Ensure systems and solutions under their purview align with the DoD Data Strategy and the DoD Component implementation plan of the DoD Data Strategy, and comply with other data-related guidance
    f. Support effective data governance for their stakeholders
    g. Identify use cases and questions that can be used for data-driven decision making
    h. Implement data management guidance and policies within their area of responsibility in coordination with the DGB
    i. Coordinate approval of data models, standards, mapping, and interface specifications with the DGB
    j. Identify and catalog common, shared datasets (e.g., master data)
    k. Identify and catalog systems creating, storing, or disposing of domain data
    l. Enable enterprise data sharing initiatives
    m. Enable, implement, oversee, and improve data interoperability among information systems
    n. Measure and report data metrics (e.g., quality, timeliness, accessibility)

   o. Audit, implement, and report compliance with the DoD Data Strategy and DoD Component implementation plan
   p. Assist with planning, programming, budgeting, and execution for data management activities
   q. Assist with the implementation of the FDS and the FDSAP.

3. Implement data governance and data management policy and guidance within their domain by working with information owners and system owners, regardless of the system in which the data originates (e.g., feeder systems) and resides (e.g., data management and analytic platforms).
4. In collaboration with their Component CDO and/or xDO, create policies for their domain.
5. Responsible for data quality with the domain.
6. Define digital policy rules for access to data based on laws, regulations, agreements, and DoD and DoD Component level policies.
7. Ensure data sharing agreements align with appropriate policy and guidance, and implement appropriate mechanisms (e.g., access controls) within the domain.
8. Appoint xDMs as required, but function as the single DGB representative for their respective stakeholders.
9. Work with the DoD Component CDO and xDOs to implement changes in policies, standards, processes, and technologies to ensure maximum execution effectiveness.
10. Participate in acquisition decisions to ensure compliance with data policies.
11. Responsible for cross-coordination with the Principal Staff Assistants (PSAs).
12. Data Initiative Identification
    a. Work with the xDOs and functional lead to identify and approve data initiatives and to prioritize initiatives based on impact to mission objectives and data analytics goals.
13. Data Identification
    a. Designate authoritative sources, unless performed at the xDO level, and ensure authoritative sources are accessible via APIs and are registered in the data catalog
    b. Assess financial impact of source selection.
14. Data Collection / Creation
    a. Approve data acquisition policies and processes
    b. Ensure that systems and platforms under their responsibility meet the data standard requirements outlined within DoD policies. When appropriate, select and approve data standards (e.g., imagery data format from sensors)
    c. Monitor the acquisition of data from existing and new data sources to ensure standards and quality requirements are met.

15. Data Preparation
    a. Define and approve the curation processes (including data quality requirements), metadata requirements, and tiered access control policies for data
    b. Define authoritative integrated data products.
16. Data Storage / Integration
    a. Designate the domain policy for data storage (e.g., platforms, cloud, backup) and security (e.g., access controls, authorizations)
    b. Validate that integrated data sources have operational APIs and are registered in the data catalog (particularly sources of authoritative data).
17. Data Maintenance
    a. Approve the process by which data is created, updated, and cleansed for conformance with defined data quality requirements for mission objectives
    b. Update access controls and data quality requirements as necessary to adapt/respond to consumer feedback.
18. Data Use
    a. Identify and manage the use and application (e.g., data analytics, visualizations, artificial intelligence, machine language) of data within domain
    b. Monitor and ensure consumer satisfaction with data and access
    c. Monitor and ensure proper authoritative data is being used for priority efforts.
19. Data Provisioning
    a. Select, approve, and oversee fielding of APIs/services that provide data access to consumers for all priority systems and data sources
    b. Identify/establish security policies and mechanisms to control data access.
20. Data Archival / Disposal
    a. Coordinate data archival and disposal periods with the DoD Component records management team to ensure that data retention schedules are implemented accordingly.

2.4 x Data Manager

Role Description
xDMs implement enterprise and domain specific data management policies and maintain the quality of the data within their scope of responsibility.

Detailed Responsibilities

1. In coordination with the Component CDO, implement appropriate functions of 44 USC §3520(c).

2. Data Initiative Identification
    a. Recommend and nominate data initiatives and data requirements that support mission objectives
    b. Identify and define analytics efforts to support mission objectives.
3. Data Identification
    a. Determine (search and identify) data sources that satisfy the data needs and requirements of missions and initiatives
    b. Nominate data and sources for data steward approval
4. Data Collection / Creation
    a. Define/propose data acquisition (acquiring of data sets and associated metadata) policies and processes
    b. Acquire data via APIs
    c. Continuously monitor, evaluate, and log data acquisitions
    d. Ensure collection policies, processes, and standards are met.
5. Data Preparation
    a. Implement transformation or curation processes
    b. Curate/process acquired data, including creation of curation metadata records.
6. Data Storage / Integration
    a. Implement user authorizations, access controls, and update permissions
    b. Select the tools, technology, and platforms for data storage
    c. Direct and manage data interoperability and integration
    d. Register data sources in the data catalog.
    e. Ensure data and sources are integrated into the data architecture, and that the data architecture is represented in appropriate DoD Component architecture documentation
    f. Oversee and/or perform data propagation/replication, high availability configuration/troubleshooting, data partitioning, partition management/optimization/tuning, and search and index creation/optimization
    g. Produce a comprehensive data dictionary for each data source that thoroughly defines and describes all data fields associated with the source data.

7. Data Maintenance
    a. Update, maintain, and refresh data as needed or assign those actions to data custodians (e.g., database administration activities)
    b. Assess, cleanse, and curate data to confirm the quality and veracity (trustworthiness) of the data to ensure data is deemed fit for access
    c. Respond to consumer feedback, particularly on data quality and data access issues
8. Data Use
    a. Direct and record the different uses (e.g., data analytics initiatives, applications) and users of the data
    b. Select the tools and technology required to apply/use the data
    c. Monitor and log data provided to consumers employing automation to the maximum extent possible
    d. Solicit, receive, and respond to data consumer feedback.
9. Data Provisioning
    a. Develop, manage, operate, and maintain API/services with appropriate security/ access controls (e.g., identity, credential, and access management)
    b. Register data source and API in the data catalog
    c. Maintain record (log) usage of API/service employing automation to the maximum extent possible
    d. Provide data to consumer in a standard format (e.g., National Information Exchange Model) as feasible and appropriate
    e. Collaborate with appropriate DoD Component stakeholders to define architecture for integrating dynamic access services including attribute services, policy rule stores, policy decision points, and policy enforcement points in support of access to tagged data
    f. Ensure exchanged data is secure (e.g., Intelligence Community – Information Security Marking, encryption).
10. Data Archival / Disposal
    a. Evaluate the conditions for data archival and disposal, and archive or dispose of data if conditions are met
    b. Map DoD and DoD Component records management policies to each data asset.

2.5 Data Custodian

Role Description
Data custodians perform mission and business data-related tasks such as collecting, tagging, and processing data, and grant individual user's access to additional information beyond that of general systems, applications, and file permissions to perform such functions, where appropriate. Data custodians must be authorized by the appropriate data steward.

Detailed Responsibilities

1. Operate and manage systems which collect, manage, and provide access to DoD Component data
2. Collect, tag, and process data
3. Ensure data quality
4. Catalog data
5. Grant individual user's access in accordance with laws, regulations, and policies
6. Implement dynamic access by linking data to appropriate digital policy rules and by developing interfaces between information systems and dynamic access services
7. Comply with applicable DoD cybersecurity standards
8. Manage data user access as prescribed and authorized by appropriate data stewards
9. Follow data handling and protection policies and procedures established by appropriate data stewards
10. Comply with all federal laws and regulations, and DoD and DoD Component policies applicable to the data in their custody
11. Data quality and data cataloging
12. Elevate concerns and insights to the xDM or data steward.

3 DoD Component Flexibility in Data Stewardship Roles and Responsibilities

In order to meet the data management needs of the DoD Component, DoD Components are given flexibility in assigning the responsibilities of these roles based on their mission requirements and needs. While DoD Components must have staff performing the "required" roles identified (i.e., CDO, data steward, xDM), they may assign "optional" role responsibilities without designating titles. Effective data management requires the execution of all responsibilities identified in this document. DoD Components may identify which positions within their DoD Component have the ability to appoint, establish, or task data management roles. As stated in Section 2.0, each DoD Component may identify the type of staff (military, civilian, contractor), the level of effort (part or full time), and the timeline for implementing data stewardship roles. Likewise, they may define reporting requirements for data stewardship roles within their organization's structure and construct.

Nothing precludes DoD Components from having staff perform other roles and responsibilities (non-data stewardship related) in addition to data management roles. At any level of this hierarchy, the person performing the data role may have other responsibilities. This depends on individual circumstances, such as the DoD Component's mission, number of personnel, number of systems, size and complexity of their data, and other items unique to a DoD Component's situation.

The DoD CDO is available to assist DoD Components with questions concerning their data management needs. The DoD CDO seeks to foster the data management community and to support DoD Components with finding ways to share best practices and lessons learned in implementing data stewardship.

4 Office of the Secretary of Defense / Principal Staff Assistants

The Office of the Secretary of Defense, Principal Staff Assistants have primary responsibility for cross-DoD Component data stewardship within their chartered areas of responsibility. The cross-DoD Component responsibilities of the PSAs are principally a policy alignment role described in this guidebook as an xDO.

5 Conclusion

The DoD Data Stewardship Guidebook establishes the structure, roles, and responsibilities required to effectively manage data as a strategic asset within a DoD Component. The guidebook is an amplification and extension of the Governance and Talent and Culture essential capabilities identified in the DoD Data Strategy. The guidebook also applies and extends the guiding principles necessary to address foundational data management activities (e.g., data quality management, metadata management, and data risk management (security, privacy, compliance)). It is a tool intended to enable a more consistent data stewardship workforce that fully exploits data for mission operations and trustworthy decision making.

6 Content for Future Versions

Items for consideration in future versions of this document or in separate guidance include:

1. Refinement of x Data Officer responsibilities
2. Refinement of x Data Manager responsibilities
3. Refinement of Data Custodian responsibilities
4. Refinement of PSA responsibilities
5. xDO structure and responsibilities
6. Mechanisms in place to ensure best practices for consistency across all DoD Components
7. References to sources for best practices
8. Privacy Act concerns
9. Identify, describe and define processes referenced in the responsibilities section of the roles.
10. Use cases / examples of best practices demonstrating when and how these best practices have led to mission success.
11. Alignment/mapping of data management terms to "IT role" terms
12. Terminology cross-walk between DoD and industry
13. DGB relationship to the broader DoD community
14. Standards and related bodies (e.g., DoD IT Standards Process, the International Standards Organizations, and U.S. Federal Standards Process) – address data standards harmonization/de-confliction across the DoD, Coalition/International, and Interagency communities.

Appendix A: Glossary

Term	Definition
Chief Data Officer	A designated senior official responsible for the management of data as an asset and the establishment and enforcement of data-related strategies, policies, standards, processes, and governance. (IC Data Management Lexicon, 2020)
Community	In relationship to data stewardship responsibilities, a group of people having an invested interest in the data sets and associated activities.
Data	A representation of facts, concepts, or instructions, such as text, numbers, graphics, documents, images, sound, or video, in a form suitable for communication, interpretation, or processing, which individually have no meaning by and in themselves. (IC Data Management Lexicon, 2020)
Data Access	The ability of a human or non-person entity to perform one or more operations on data, typically via service endpoints and APIs. These operations may include the ability for data to be searched, retrieved, read, created, updated, deleted, manipulated, and executed. (IC Data Management Lexicon, 2020)
Data Asset	Data 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. (IC Data Management Lexicon, 2020)
Data Custodian	May perform mission and business data-related tasks such as collecting, tagging, and processing data, and may grant individual user's access to additional information beyond that of general systems, applications, and file permissions to perform such functions, where appropriate. The data custodian does not assume the legal or policy roles of the DoD Component. (IC Data Management Lexicon, 2020)
Data Governance	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 across a Component to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives. (IC Data Management Lexicon, 2020)

Data Governance Board (DGB) A decision- and/or policy-making board of senior managers, chaired by the CDO, that is responsible for the highest tier of data governance in a Component. The DGB oversees or manages data governance initiatives (e.g., development of policies or metrics), issues, and escalations. The DGB monitors results to ensure that the Component receives the desired outcomes and business value from data management activities. This may also be called a Data Council, Executive Data Council or Data Executive Council. For the purposes of this document the body has been called a board. (IC Data Management Lexicon, 2020)

Data Lifecycle A conceptualization of a birth-to-death 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. (IC Data Management Lexicon, 2020)

Data Lifecycle Management Establishment and execution of policies and interconnected processes for managing data throughout the data lifecycle to support data management functions, such as data governance. (IC Data Management Lexicon, 2020)

Data Management Development and execution of plans, policies, programs, and practices (4Ps) that acquire, control, protect, and enhance the value of data assets throughout the lifecycle, led or performed by professionals following established disciplines and functions. (IC Data Management Lexicon, 2020)

Data Management Plan A plan that documents how specific data is collected, processed, used, and curated in order to facilitate long-term data management decisions and actions. It typically includes topics such as:

i. Description of the data to be collected/created
ii. Authority under which the data is collected
iii. Standards/methodologies for data collection and management
iv. Ethics and Intellectual Property concerns or restrictions
v. Plans for data sharing and access
vi. Strategy for long-term preservation of the data.

(IC Data Management Lexicon, 2020)

Data Management Strategy Selected courses of action setting the direction for data management within the enterprise, including vision, mission, goals, principles, policies, and projects. (DAMA Dictionary, 2nd Edition)

Data Quality The degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use. (IC Data Management Lexicon, 2020)

Data Steward Data steward responsibilities are assigned to specific personnel across a multi-level data stewardship hierarchy. Whether represented by a single employee or by responsibilities distributed through an organizational hierarchy, data stewards are legally accountable across the data lifecycle on behalf of the Component for:

a. Establishing protection, sharing, and governance guidelines for data and datasets within an assigned subject area
b. Maintaining data names, business definitions, data integrity rules, and domain values within an assigned subject area
c. Complying with legal and policy requirements and conformance and data policies and data standards
d. Ensuring application of appropriate security controls
e. Analyzing and improving data quality
f. Identifying and resolving data related issues.

(IC Data Management Lexicon, 2020)

Data Stewardship The formal, specifically assigned, and entrusted accountability for business (non-technical) responsibilities ensuring effective control and use of data and information resources. (DAMA Dictionary, 2nd Edition)

Domain A specific unit of a DoD Component and/or a functional area in which the same type of data is usually generated, used, or shared. Examples include, but are not limited to Mission Areas, Joint Capability Areas, and lines of business. (Amplified from Merriam-Webster.com)

Domain Data Data generated, used, or shared within a specific domain.

Echelon A unit or group acting in a disciplined or organized manner, which can be at different levels of a DoD Component, but is below the headquarters level. (Amplified from Merriam-Webster.com)

Enterprise The scope of an organization as defined by that organization based on a purpose or point of view. An enterprise may be a business, not-for-profit, government agency, or educational institution. An enterprise has a purpose, goals, and objectives. (DAMA DMBoK, 2nd Edition)

For the purpose of this document, except when referencing the DoD Data Strategy or Mission Areas, enterprise refers to a DoD Component as identified:

a. Office of the Secretary of Defense
b. Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff
c. Combatant Commands
d. Office of the Inspector General of the Department of Defense
e. Military Departments
f. Defense Agencies

g. DoD Field Activities
h. Other organizational entities, which includes the National Guard Bureau

Enterprise Data Data that is used, shared, or generated with a particular point of view or perspective, generally DoD Component-wide, DoD-wide, or a functional area that involves many or all of the DoD Components. (Amplified from DAMA Dictionary, 2nd Edition)

Headquarters Managerial and administrative center of a DoD Component. (Amplified from Merriam-Webster.com)

Master Data Data that provides the context for business activity data in the form of common and abstract concepts that relate to the activity. It includes the details (definitions and identifiers) of internal and external objects involved in business transactions such as customers, products, employees, vendors, and controlled domains (code values). (DAMA Dictionary, 2nd Edition)

Maturity The quality and/or state of development of either data or the data management activities, processes, and tools being used to perform data management functions. (Amplified from Merriam-Webster.com)

Appendix B: Acronyms

Acronym	Definition
API	Application Programming Interface
CCMD	Combatant Command
CDO	Chief Data Officer
DAFAs	Defense Agencies DoD and Field Activities
DoD	Department of Defense
DGB	Data Governance Board
FDS	Federal Data Strategy
FDSAP	Federal Data Strategy Action Plan
IC	Intelligence Community
JCA	Joint Capability Area
MILDEPS	Military Departments
OSD	Office of the Secretary of Defense
USC	United States Code
xDO	“x” Data Officer
xDM	“x” Data Manager

Appendix C: DoD Data Strategy Summary

Focus Areas: The strategy emphasizes the need to work closely with users in the operational community, particularly the warfighter. Initial areas of focus include:

1. Joint All Domain Operations – using data for advantage on the battlefield
2. Senior Leader Decision Support – using data to improve DoD management
3. Business Analytics – using data to drive informed decisions at all echelons

Eight Guiding Principles that are foundational to all data efforts in the DoD:

1. Data is a Strategic Asset – DoD data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage.
2. Collective Data Stewardship – DoD must assign data stewards, data custodians, and a set of functional data managers to achieve accountability throughout the entire data lifecycle.
3. Data Ethics – DoD must put ethics at the forefront of all thought and actions as it relates to how data is collected, used, and stored.
4. Data Collection – DoD must enable electronic collection of data at the point of creation and maintain the pedigree of that data at all times.
5. Enterprise-Wide Data Access and Availability – DoD data must be made available for use by all authorized individuals and non-person entities through appropriate mechanisms.
6. Data for Artificial Intelligence Training – Data sets for A.I. training and algorithmic models will increasingly become the DoD's most valuable digital assets and we must create a framework for managing them across the data lifecycle that provides protected visibility and responsible brokerage.
7. Data Fit for Purpose – DoD must carefully consider any ethical concerns in data collection, sharing, use, rapid data integration as well as minimization of any sources of unintended bias.
8. Design for Compliance – DoD must implement IT solutions that provide an opportunity to fully automate the information management lifecycle, properly secure data, and maintain end-to-end records management.

Four Essential Capabilities necessary to enable all goals:

1. Architecture – DoD architecture, enabled by enterprise cloud and other technologies, must allow pivoting on data more rapidly than adversaries are able to adapt.

2. Standards – DoD employs a family of standards that include not only commonly recognized approaches for the management and utilization of data assets, but also proven and successful methods for representing and sharing data.

3. Governance – DoD data governance provides the principles, policies, processes, frameworks, tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition.

4. Talent and Culture – DoD workforce (Service Members, Civilians, and Contractors at every echelon) will be increasingly empowered to work with data, make data-informed decisions, create evidence-based policies, and implement effectual processes.

Seven Goals (aka, VAULTIS) we must achieve to become a data-centric DoD:

1. Make Data Visible – Consumers can locate the needed data.
2. Make Data Accessible – Consumers can retrieve the data.
3. Make Data Understandable – Consumers can recognize the content, context, and applicability.
4. Make Data Linked – Consumers can exploit data elements through innate relationships.
5. Make Data Trustworthy – Consumers can be confident in all aspects of data for decision-making.
6. Make Data Interoperable – Consumers have a common representation/comprehension of data.
7. Make Data Secure – Consumers know that data is protected from unauthorized use/manipulation.

Appendix D: References

1. Department of Navy (DoN), “Data Management CONEMP v 1.0.”

2. United States Army, “Data Management Program Roles & Responsibilities v10.”

3. The Intelligence Community Data Management Lexicon, Office of the Director of National Intelligence, January 2020.

4. 2020 DoD Data Strategy, September 30, 2020.

5. Deputy Secretary of Defense Memorandum, “Creating Data Advantage,” May 5, 2021.

6. DAMA Dictionary of Data Management, 2nd Edition.

7. Merriam-Webster.com