DAF CHIEF DATA AND AI OFFICE

DEPARTMENT OF THE AIR FORCE DATA STRATEGY

Controlled by: Department of the Air Force
Controlled by: Chief Data and AI Office
Distribution/Dissemination Control: DISTRIBUTION A
POC: SAF.CND.Chief.Data.And.AI.Office.Workflow@us.af.mil

Cleared for open publication ▪ April 17, 2026 ▪ Department of the Air Force

Contents

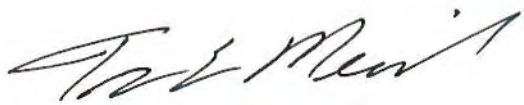
FOREWORD

To prevail in an era of persistent strategic competition, we must achieve decision advantage. Accomplishing this requires treating data as a strategic asset, essential for integrated deterrence and cohesion with the Joint Force.

For too long, fragmented and siloed data has hindered our operational agility. The Department of the Air Force Data Strategy provides the framework to correct this by shifting from legacy architectures to a decentralized data management approach, treating data as a product to be securely and rapidly shared. Building a data-centric enterprise will empower the total force to leverage data for mission success.

Executing this strategy is a national security imperative. I expect leaders at every echelon to drive this change and break down the organizational barriers to its success.

By providing our warfighters with trusted data at the speed of mission, we equip them to deter and, if necessary, prevail. The time for action is now.



Troy E. Meink
Secretary of the Air Force

EXECUTIVE SUMMARY

This document establishes the Department of the Air Force's (DAF) strategic direction to advance data modernization and achieve informational readiness. Guided by Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure (VAULTIS) data principles and Department of Defense (colloquially recognized as the Department of War (DoW)) guidance including the 2026 Data Strategy for the Department of War (pending) and the 2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, this DAF Data Strategy outlines a robust and agile data ecosystem to empower decision-makers at all echelons. The DAF will address key challenges in the current data architecture by adopting a decentralized, domain-driven approach to data management. Data will be treated as a strategic asset and discoverable and consumable authoritative data will be accessible via self-service tools. A decentralized approach to data management will enhance data transparency, increase interoperability, improve decision advantage, and promote Artificial Intelligence (AI) readiness across the DAF.

The DAF Data Strategy establishes three core pillars: Streamlined Data Discovery and Accessibility, Enhanced Data Trust and Interoperability, and Increased Data-Driven Decision Making. The pillars detail key outcomes that will be achieved by modernizing the DAF's data landscape. Four building blocks for enterprise lifecycle data management success provide the necessary foundation to actualize these core pillars: Governance and Responsibility, Data Readiness, a Data Mesh Environment, and a Data-Centric Workforce.

This document serves as both a foundation for immediate action and a guide to achieving data readiness that will evolve in line with organizational priorities into 2031. The successful execution of this strategy will be instrumental in enhancing warfighter effectiveness, improving operational efficiency, and ensuring the DAF maintains its competitive edge in an increasingly data-centric world.

ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
DAF CDAO	Department of the Air Force Chief Data and Artificial Intelligence Officer
DCWF	DoD Cyberspace Workforce Framework
DME	Data Mesh Environment
DoD	Department of Defense
DoW	Department of War
ICAM	Identity, Credential, and Access Management
IC	Intelligence Community
VAULTIS	Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure

INTRODUCTION

The Data Imperative

The DAF depends on seamless integration and utilization of data as a strategic asset to execute its core functions. Mastery of data drives the DAF's competitive advantage, accelerates the integration of AI capabilities, and ensures a decisive response to evolving threats.

Stakeholders

Stakeholders of the DAF Data Strategy span all echelons of the enterprise. The DAF CDAO governs the implementation of the strategy, working closely with DAF organizations and assigned DAF Data Officers to facilitate sound enterprise decision management oversight. Data management offices and compliance teams at the Secretariat, Functional, Major and Field Command, Direct Reporting Unit, and Air National Guard-levels ensure enterprise data management, data quality, security, privacy, and adherence to data management regulations. This Strategy applies to all civilian employees and uniformed members of the United States Air and Space Forces, Air Force Reserve, Air National Guard, and those with a contractual obligation to abide by the terms of DAF issuances.

Scope

The DAF Data Strategy applies to all data generated and managed across the DAF enterprise including structured, semi-structured, and unstructured data at all classification levels and security protection levels (Unclassified, Controlled Unclassified Information, Secret, Top Secret, and Special Access Programs). It orients the DAF towards a highly interoperable enterprise data landscape that enables effective integration within the DAF, with external DoW and Federal data ecosystems, and with allied and coalition mission partner environments. This strategy recognizes that certain data domains operate under specific authorities and governance structures. The Office of the Director of National Intelligence governs intelligence production data and systems owned by the Intelligence Community (IC) in accordance with Section 3024 of Title 50 United States Code and falls outside the purview of this strategy. Where appropriate, implementation of this strategy will be coordinated with IC governance to ensure complementary approaches without duplication of authority.

Guiding Principles

The guiding principles support the courses of action and goals outlined in the 2026 National Defense Strategy, the 2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, and the 2026 Data Strategy for the Department of War (pending), emphasizing data's critical role in sustaining a competitive advantage and enacting effective AI integration.

VAULTIS DAF Data: The DAF will continue to make its data more VAULTIS. This means DAF data must be inherently Visible and Accessible; it will be discoverable through comprehensive cataloging with metadata and readily available to authorized users. To enable effective analysis, data must be Understandable through clear documentation and Linked via architecture that supports seamless integration.

The data will be Trustworthy, with its quality and reliability ensured through infrastructure that tracks its lineage, provenance, and pedigree. It will be Interoperable, employing a common representation to facilitate exchange of data between systems, and above all, it must remain Secure, protected by robust measures from unauthorized discovery, access, use, or destruction.

Decentralized Data Management: A decentralized approach to data management distributes the responsibility for ensuring data is VAULTIS to organizational structures called data domains. The decentralized data model empowers data domains, which are organizational units led by the subject matter experts closest to the information. Each domain holds the authority and responsibility for ensuring its data meets both enterprise and mission-specific standards. This approach leverages expertise where it lives to guarantee data is fit-for-purpose, while giving domains the flexibility to use the infrastructure that best meets their unique requirements.

Foundational Data Governance: Effective data management and orchestration within the DAF relies on strong data governance. Policies and standards create the framework for responsible and sustainable data use. Data domains provide structures of accountability, oversight, and advocacy to ensure data production and use within the domain adhere to relevant policies and standards. Each DAF data domain must implement its own governance structures and will be led by a Domain Principal. This General Officer or Senior Executive Service civilian represents the domain in enterprise governance forums and exercises their authorities and influence to ensure data sources in their respective domain are appropriately resourced and matured. Enterprise data governance structures balance autonomy with alignment, ensuring the prioritization of enterprise objectives through support and oversight of DAF data domains. Centralized governance harmonizes decentralized data management practices across the DAF, ensuring a cohesive data landscape, common data representation, and minimization of data inconsistencies.

Empowered and Equipped Workforce: Just as security is the responsibility of every member of the DAF workforce, executing data-centric operations requires all DAF personnel to understand and fulfill their role with respect to data. Empowering and equipping the workforce includes providing resources to develop data competencies, adopting formal data work roles with defined responsibilities, establishing governance, providing training resources, and considering human systems integration principles, including user experience and workflow optimization. Commanders and Principals at all echelons require supporting resources and policy direction to prioritize data centricity alongside other mission requirements. The DAF will resource data initiatives with visibility and accountability to build trust and enable collaboration across organizational boundaries.

VISION

Vision Statement

Enabling the secure sharing of discoverable and consumable authoritative DAF data at the speed of mission.

To enable the secure sharing of authoritative DAF data at the speed of mission, we will adopt a decentralized data management paradigm, as depicted in Figure 1, aligned with the 2024 DoD Data Mesh Reference Architecture. This modern approach consists of two primary elements: a robust framework for governance, and a streamlined layer of enterprise technology.

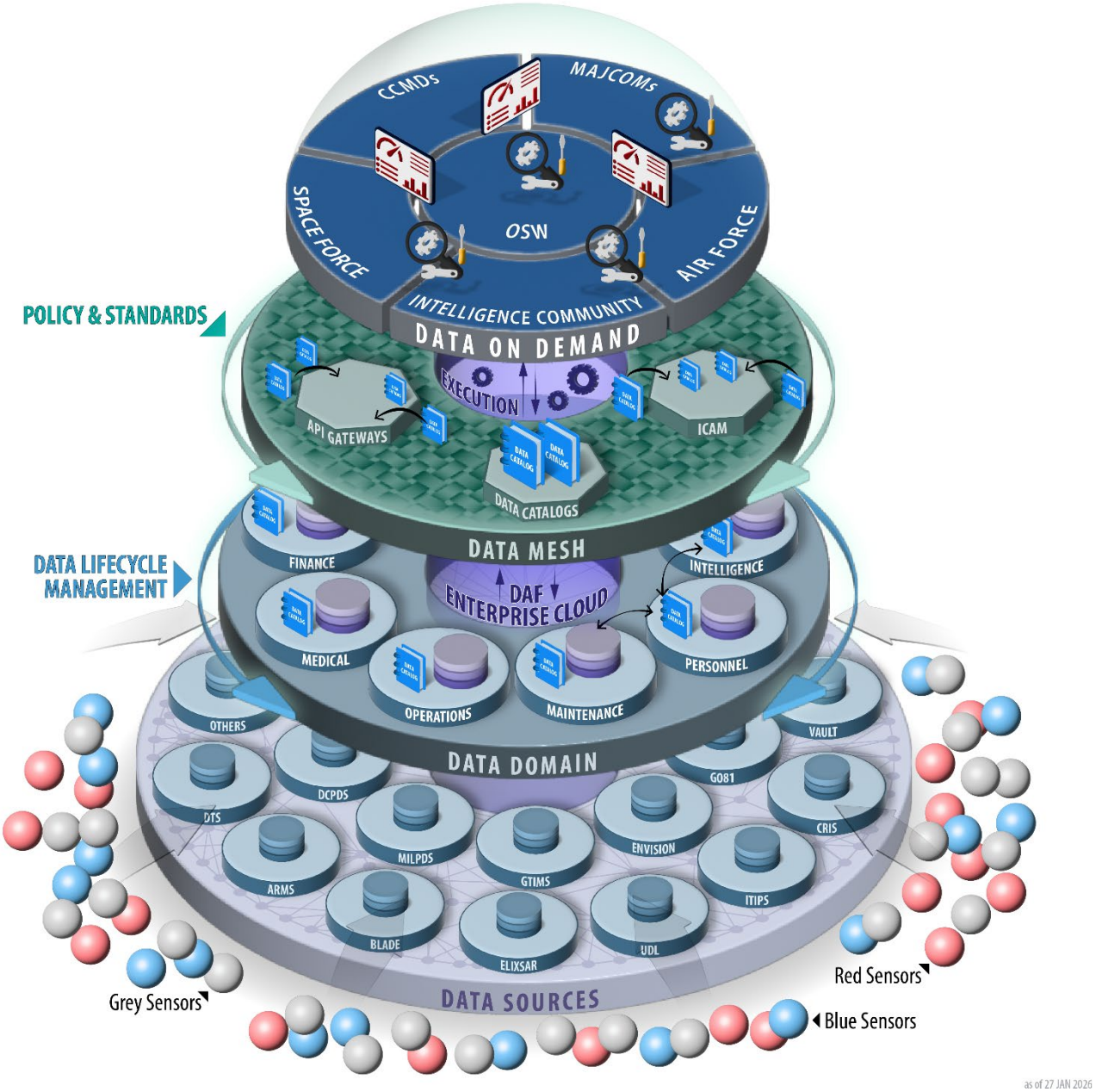


FIGURE 1: VISION FOR THE DAF DATA ARCHITECTURE

Under this model, accountability for data is pushed to the mission edge through data domains. These domains, led by the experts closest to the information, are responsible for producing valuable, relevant, and high-quality data products for the enterprise. Treating data as a product ensures that data assets are deliberately designed and iteratively curated to meet user needs and requirements.

At the enterprise level, a centrally funded enterprise data catalog will serve as the single front door for all data consumers. This self-service catalog will provide access to domain-curated data products, directly increasing value, trust, and quality assurance of DAF data as a strategic asset.

PILLARS

Three core pillars describe the expected outcomes that will be realized across the DAF by implementing the DAF Data Strategy. They support efficient and effective mission achievement in every domain.

Pillar 1: Streamlined Data Discovery and Accessibility

Objective: Reduce the time required to share data between domains and increase the percentage of DAF data that is readily accessible to authorized users.

- **Automated Metadata Tagging:** Data domains ensure automated metadata tagging and publishing services for every DAF data source.
- **Enterprise Data Catalog:** A self-service DAF data catalog, functionally managed by the DAF CDAO, makes data from every domain discoverable to the enterprise in accordance with need-to-know security requirements. This DAF data catalog spans all classification levels, allowing for semantic search of data assets and products and providing access to API endpoints for immediate data use. Data published to the catalog is appropriately tagged and is accompanied by contextualizing information such as standardized data dictionaries.
- **Standardized APIs:** DAF API standards simplify data sharing within and across domains. API management tools are integrated with the DAF data catalog, enabling efficient data discovery and access. Legacy systems incapable of API provisioning are appropriately matured or leverage alternative, reasonable, and standardized methods for efficient data sharing.
- **Enterprise ICAM:** User identities and access are securely managed at the enterprise level, integrating security controls into API gateways and data catalogs. Data is protected at rest, in motion, and in use through maximum automation and enforcement of data security controls

Pillar 2: Enhanced Data Trust and Interoperability

Objective: Increase the interoperability of data for cross-functional use and increase the percentage of DAF data assets that have documented quality metrics.

- **Establish Standards:** Enterprise and data domain-specific standards are established for how data assets and associated metadata will be tagged.
- **Semantic Services**: Semantic search and discovery capabilities enable users to find data based on meaning rather than just keywords.

- **Data Modeling and Ontology:** A common data ontology aligned with standards is designed and implemented to improve data understanding and trust. All DAF domain ontologies conform to these DoW standards to ensure semantic interoperability across the enterprise.
- **Quality Verification:** Automated data quality standards are implemented. Data quality rules and thresholds are established at both enterprise and domain levels. Data observability and monitoring tools provide continuous visibility into data pipeline health and quality metrics.
- **Lineage, Provenance, and Pedigree:** Comprehensive data tracking for DAF data assets is established. Data provenance tracks the origin of data (source system or organization). Data lineage traces data throughout its lifecycle, including systems the data moves through and transformations applied. Data pedigree assesses the quality of the origin and lineage, including accuracy, completeness, and compliance with established standards and authorities. Comprehensive data tracing will determine the fitness of the data asset and ensure data is accurate, reliable, and trustworthy.

Pillar 3: Increased Data-Centric Decision Making

Objective: Increase the utilization of data in all DAF decision-making processes.

- **Governance:** Data governance bodies develop or implement data standards, policies, and practices supporting the ability to manage improvements to data reliability and lineage, operational efficiency, and decision making.
- **Data Product Approach:** Data assets are transformed into data products, which are deliberately designed and iteratively curated to be valuable and relevant to users. Data products are developed and managed to resolve differing data standards and formats without data loss of fidelity, precision, or accuracy to enable maximum reusability across platforms and mission contexts.
- **Data Analytics Enablement:** VAULTIS DAF data goals support the transformation of raw data into actionable insights. Policies, processes, and protocols for effective data analytics are upheld in partnership with the DAF Chief Analytics Officer.
- **Data Acumen Programs:** Data acumen programs aligned with the DoW Cyber Workforce Framework promote a data-centric culture and empower leaders to understand, communicate, and analyze data in context and therefore make data-informed decisions at all echelons.

CHALLENGES

The DAF faces significant challenges in utilizing its vast data resources, jeopardizing its ability to keep pace with near-peer competitors. These challenges span governance and oversight, technical implementation, and organizational and resourcing barriers.

The DAF's current data management architecture is fragmented and inconsistent. Insufficient metadata tagging and data cataloging have rendered most of the DAF's data undiscoverable and inaccessible. Fragmented visibility and transparency toward enterprise funding for data initiatives erode collaboration and trust. DAF personnel rely on centralized data platforms to access consumable data, often limiting data access

to incomplete, use-case-driven data feeds. Widespread point-to-point data connection practices cause mission delays, unnecessary data duplication, and heightened security concerns. A lack of data readiness at the domain level inhibits comprehensive information management, and therefore informed decision-making, at the enterprise level.

Governance and Oversight Deficiencies: The maturity of DAF data governance processes is disjointed and inconsistent, resulting in fragmented data management and a lack of effective oversight.

- Lack of metadata standardization. Lack of requirements for curated data to meet standards and maximize interoperability across systems and missions.
- Absence of standardized web-based, machine-readable, open format approaches (e.g. common interfaces) that maximize reuse wherever operationally and technically possible.
- Insufficient standards and enforcement for data sharing and discovery, including a lack of requirements for API implementation at the data source level.
- Inability to measure data readiness and effectiveness.
- Insufficient customer service orientation in data support.
- Insufficient knowledge and understanding of required data standards during acquisitions, beginning with requirements definition.

Technical Implementation Gaps: Critical technical components for effective data management are missing in the DAF's current architecture.

- Lack of an API management capability to control access and distribution of APIs based upon ICAM policy. Must establish continuous authentication, privilege, and encryption to protect against risk and threat in a complex DAF data environment. *Note: API management is separate from user authentication and requires dedicated infrastructure*.
- Lack of a self-service enterprise data catalog.
- Lack of data retention/lifecycle policy enforcement.
- Lack of performance metrics and observability tools for data services.
- Absence of data standardization, including normalized data definitions and common data features and standards across systems.

Organizational and Resourcing Barriers: Resistance to change, limited data acumen, insufficient leadership support, and funding challenges impede the adoption of effective DAF data management optimization.

- Insufficient senior-leadership prioritization of data management practices
- Lack of supporting resources, policy, and manpower allocation to enable Principals and Commanders to prioritize data readiness alongside other mission needs.
- Competing interest of readily available data visualization over the quality of the underlying data leads to flawed insights, poor decision-making, and a loss of trust
- Data accuracy challenges stemming from human error during data input, creating far-reaching impacts particularly for human resources and personnel data.
- Excessive and complex documentation requirements, making it difficult for practitioners to stay current with evolving guidance.

- Limited availability and inventory of data ontology, architecture, and engineering subject matter experts working across both programs of record and non-standard systems to enable proper data architecture implementation.

OPERATIONALIZING THE STRATEGY

The vision of the DAF Data Strategy will be actualized through four critical building blocks: Governance and Responsibility, Data Readiness, a Data Mesh Environment, and a Data-Centric Workforce. These building blocks are foundational for achieving the three pillars of this strategy. They will enable strategic concepts to become operational realities by supporting mission-focused and user-driven data initiatives.

FIGURE 2: DAF DATA STRATEGY OPERATIONAL VIEW

Governance and Responsibility

The DAF provides a robust body of policy and governance to serve as the foundation for modernizing DAF data architecture and management practices. Effective governance adheres to federal and DoW guidelines while remaining agile to accommodate changes and maintain alignment with strategic objectives. Governance-driven strategy will align efforts and priorities across the DAF by outlining outcomes and architectural roadmaps without prescribing specific technical solutions. Policy and implementation realize strategic visions. The DAF will continue to produce data policies that guide the ethical and effective management and use of data and will critically assess existing policies to ensure alignment with DoW and DAF strategic objectives. Within a decentralized data management paradigm, data domains will establish their own governance bodies to assure a roster of key data management personnel, ensure effective cross-communication, and garner feedback. Data Domain Principals and governance bodies will ensure the data sources within the domain comply with DoW and DAF policies. DAF data leaders will actively participate in existing data governance structures, promoting shared accountability for enterprise data readiness.

Data Readiness

The DAF will achieve data readiness by treating data as a strategic asset, akin to personnel and materiel, to enable faster and better-informed decisions. Readiness is achieved when data is suitable for its intended use and meets the needs and requirements of users. Enterprise and data domain-specific data governance bodies must be established to foster a collaborative landscape to ensure standards are prioritized and developed to be clear, achievable, and supportive of mission outcomes. DAF CDAO will provide oversight of enterprise data readiness to monitor the compliance of data domains with existing standards, ensuring that leaders and decision-makers have critical insight into the readiness of the DAF's data assets.

Data domains are responsible for defining any relevant domain-specific standards for data readiness and for appropriately maturing all DAF data sources within their respective domains. Data Source maturity includes:

- Data Governance – Data access and approval processes are largely automated while maintaining appropriate human oversight for sensitive decisions.
- Data Trust – Data platforms automatically generate and provide quality metrics for all data assets. The DAF will establish life cycle management to track, report, and improve quality metrics across all data sources.
- Data Discovery – Automated workflows provision metadata from all data assets to domain and enterprise catalogs, with appropriate security controls for classified or sensitive data.
- Data Provisioning – Data sources are enabled with standardized data provisioning capabilities such as APIs.
- Data Collaboration – Functional taxonomies define shared data standards and maintain clear data definitions and contextual documentation to prevent misinterpretation.

To achieve comprehensive data readiness as a Military Department, the data published from each matured data source to the enterprise must be comprehensible and suited for effective use by data consumers including analysts, decision-makers, and non-person entities such as AI models. Data domains will be responsible for curating valuable, relevant, and usable data products.

Data Mesh Environment

Adopting a decentralized approach to data management will align the DAF to a data mesh paradigm. The DAF CDAO will provide a thin, streamlined layer of enterprise technology to make DAF data discoverable and sharable. This suite of self-service tools, called the Data Mesh Environment (DME), will function as a data product marketplace, enabling data producers and consumers to publish and access DAF data in a secure and interoperable environment. Key features of the DME will include:

- A virtually federated enterprise data catalog that aggregates metadata from domain catalogs without centralizing data storage.
- Data asset search tools for fast, relatable, and semantically understandable searching of DAF data, leveraging natural language processing and ontology-based search capabilities.
- API gateway management infrastructure for handling and routing API requests, with built-in monitoring, rate limiting, and security controls.
- ICAM capabilities for secure data sharing, integrated with enterprise identity management systems to provide role-based access control.

Data domains will be responsible for publishing their data products to the DME. Data domains must populate this collaborative environment with high quality data that complies with all relevant standards for data readiness to ensure the DAF's data-centric decision advantage across all missions and functions.

Data-Centric Workforce

The DAF will cultivate a data-centric workforce through strategic investment and comprehensive initiatives. A data-centric workforce possesses the knowledge and skills necessary to read, work with, analyze, and communicate with and about data effectively. Data acumen encompasses understanding data sources, recognizing data quality issues, applying appropriate analytical methods, and making evidence- based decisions. The DAF will develop data acumen competencies based on role to ensure basic data awareness for all personnel and advanced analytical capabilities for data and analytics professionals. The DAF will leverage learning platforms and online resources, making data acumen materials readily accessible to all personnel.

Strategic workforce planning aligned with DCWF work roles, including regular assessments of DAF data workforce needs, will drive targeted recruitment and training strategies, aligning workforce development initiatives to long-term data management strategic objectives. The DAF data workforce will actively contribute to a data-centric environment by championing data acumen at every echelon. Data domains are responsible for leveraging the resources provided by the DAF to understand and implement data management best practices.

CALL TO ACTION

The DAF Data Strategy establishes the strategic direction for a data-centric DAF, recognizing data is a strategic asset essential for achieving decision dominance in the modern information environment. Embracing the VAULTIS principles, domain-oriented decentralized data management, and federated governance will empower the DAF workforce to leverage data effectively for improved mission effectiveness. By implementing this strategy, the DAF will transform data into a decisive advantage across all mission sets.

Modernizing the DAF data ecosystem is an urgent requirement. Evolving threats and near-peer competition require timely and decisive action. This strategy will realize data transparency in the DAF, correcting historical drift in priorities and resourcing to ensure that VAULTIS data, accessible across domains, is effectively leveraged to achieve force readiness and lethality. The DAF commits to a phased implementation approach with clear milestones and accountability. The DAF requires secure, accessible, and trustworthy data to defend the homeland, deter aggression, and prevail in conflict.

REFERENCES[1]

DoD Directive 8140.01, *Cyberspace Workforce Management*, October 5, 2020

DoD Instruction (DoDI) 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*, December 21, 2021

DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*, June 24, 2020

DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*, December 5, 2017

DoD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program*, February 15, 2023

Office of the Secretary of War, *2026 National Defense Strategy*, January 23, 2026, available at https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF

Office of the Secretary of Defense, *2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy*, June 27, 2023, available at https://media.defense.gov/2023/nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf

Office of the Secretary of Defense, *DoD Data Strategy: Unleashing Data to Advance the National Defense Strategy*, September 30, 2020,available at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

Office of the Secretary of Defense, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy*, March 2022, available at https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf

Office of the DoD Chief Digital and Artificial Intelligence, *Data Mesh Reference Architecture, Version 2.6*, March 2024, available at https://media.defense.gov/2024/Mar/15/2003414274/-1/-1/1/dmra_paper.PDF

Office of the Director of National Intelligence, *Intelligence Community Data Management Lexicon*, May 2024, available at https://www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf

Air Force Policy Directive 90-70, *Enterprise Data Management*, February 13, 2020

Air Force Instruction 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*, May 23, 2018

Department of the Air Force Instruction 90-7001, Enterprise *Data Sharing and Data Stewardship*, April 22, 2021

1 Footnote: The Data Strategy for the Department of War is pending release. A pre-publication draft was reviewed to ensure alignment in publication of this DAF Data Strategy

DEFINITIONS

Unless stated otherwise, the following definitions are taken from the OSD CDAO-approved data lexicon at www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf

Authoritative Data: Data provided by an authoritative source.

Authoritative Source: A source of data or information that is recognized by members of a Community of Interest, as defined in Committee on National Security Systems Instruction (CNNSI) 4009, 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 (SMEs) validate that the data is authoritative, and data management ensures that data from the authoritative source is provided to users and is current.

Catalog: A curated collection of metadata about resources (e.g., datasets, data services in the context of a data catalog), usually arranged systematically.

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.

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 to search, retrieve, read, create, update, delete, manipulate, and execute data.

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 or system output files, and records.

Data Acumen: The ability to sufficiently understand, analyze, reason, communicate, and make decisions and judgments with and about data in context.

Data Consumer: A person or NPE that receives data (e.g., on a screen, in a report, through a query, or via a machine-to-machine interface), uses the data for a specific purpose, and can be affected by its quality

Data Curation: The active maintenance of data throughout its lifecycle to ensure levels of readiness for current and future use. Data curation activities involve continuously working with data creators and users, enhancing discovery and retrieval, supporting research and data correlation, ensuring data quality, protection and accessibility, and adding value to data (e.g., collection building, adding metadata, providing search mechanisms).

Data Domain: A collection of data representing key concepts across a specific mission area that is usually identifiable via recognizable governance or authoritative bodies.

Data Fabric: A design concept that serves as a federated and integrated layer (fabric) of data and connecting processes for sharing information through interfaces and services to discover, understand, and exchange data with partners across all applications, domains, echelons, and security levels.

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 across an IC element to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives.

Data Interoperability: The ability of systems and services that create, exchange, and consume data to have clear, shared expectations (e.g., conventions, standards, policy) for the contents, context, and meaning of that data across varying platforms and security domains.

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 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.

Data Management: The 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 tradecraft professionals following established disciplines and functions.

Data Mesh: A decentralized organizational and technical approach to sharing, accessing, and managing data in large-scale environments within or across organizational boundaries. This approach links disparate sources through centrally managed sharing and governance guidelines. The result is a domain-oriented, federated approach where data is created and consumed as a product.

Data Producer: This term is synonymous with Data Provider.

Data Provider: An organization or person who initially creates or provides data on behalf of the Originating Element. This may be a Collection Steward, Analytic Production Steward, Data Custodian, or an external data source functioning on behalf of the Originating Element.

Data Quality: The degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use.

Data Security: The ability to protect data resources from unauthorized discovery, access, use, modification, and/or destruction. Secure data-sharing relies on several key functions: data identification, categorization, and labeling; entitlement management; and policy establishment.

Data-Sharing: The practice of providing access to data resources to multiple users, applications, or organizations while maintaining the fidelity and integrity of the data. This includes the technologies, practices, legal frameworks, and cultural elements that ensure data is available to any entity with a need-to- know basis and proper access permissions while protecting it from unlawful or improper use.

Data Standards: Specifications, sets of rules, methods, terminologies, or guidance, approved by a recognized body to enable how data is created, stored, exchanged, managed, or processed in a common and repeatable way to facilitate data interoperability. Data standards codify the representation, format, definition, structuring, tagging, transmission, manipulation, use, or management of data.

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.

Metadata: Literally, "data about data"; administrative or descriptive data attributes that are consistent across mission and business disciplines, domains, and data encodings and are used to improve business or technical understanding of data and data-related processes.

Semi-structured Data: Data that has elements of both unstructured and structured data. For example, a Microsoft Word document is generally considered to be unstructured data, but with the addition of metadata tags used to enable discoverability, the data is now semi-structured. Other types of semi-structured data formats include: Extensible Markup Language (XML), JavaScript Object Notation (JSON), email, and formats based on Electronic Data Interchange (EDI) standards (e.g., X12, Electronic Data Interchange for Administration, Commerce, and Trust (EDIFACT), Organization for Data Exchange by Tele Transmission in Europe (ODETTE)).

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.

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.

DAF CHIEF DATA AND AI OFFICE

DATA–DRIVEN | AI–POWERED | MISSION–READY