

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

**DEPARTMENT OF THE AIR FORCE
INSTRUCTION 90-7001**



22 APRIL 2021

Special Management

**ENTERPRISE DATA SHARING & DATA
STEWARDSHIP**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/COS

Certified by: SAF/COS
(Mr. Martin Akerman)

Pages: 15

This instruction implements Air Force Policy Directive (AFPD) 90-70, *Enterprise Data Management*, in accordance with the Open, Public, Electronic, and Necessary Government Data Act (OPEN Government Data Act) as codified in Title 44 United States Code (USC) Sections 3502, 3504(b), 3506(b) and (d), and 3520; Department of Defense Directive (DoDD) 8000.01, *Management of The Department of Defense Information Enterprise (DoD IE)*; Department of Defense Instruction (DoDI) 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*; DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*. This Department of the Air Force Instruction (DAFI) applies to all individuals at all levels who prepare, manage, review, disseminate or use Department of the Air Force data, including all civilian employees and uniformed members of the United States Air Force, Air Force Reserve, and United States Space Force, and those with a binding agreement or contractual obligation to abide by the terms of Department of the Air Force issuances. This DAFI identifies Enterprise Data Management (EDM) guidelines for leveraging data as a strategic asset to meet United States Air Force and United States Space Force mission requirements. It also establishes the Department of the Air Force policy to achieve enterprise-wide data visibility and accessibility, and addresses standards for data sharing under the direction of the Chief Data Officer (SAF/CO). This publication may be supplemented at any level, but all supplements that directly implement this instruction must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. This Instruction requires the collection and/or maintenance of information protected by the Privacy Act of 1974 authorized by DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*. The applicable SORNs, DUSDC 01, 85 FR 15150

(Defense Repository for Common Enterprise Data) and DUSDC 02, 85 FR 16620 (Forms and Account Management Service) are available at: <http://dpclo.defense.gov/Privacy/SORNs.aspx>. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the OPR using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor’s commander for non-tiered compliance items.

Chapter 1

ENTERPRISE DATA MANAGEMENT AND DATA SHARING

1.1. Background. Data is a strategic asset that must be properly managed to be a force multiplier to improve United States Air Force and United States Space Force mission effectiveness, readiness, lethality, and fiscal responsibility. Data and the information derived from it belong to the Department of the Air Force and are not owned by a particular application or subordinate Department of the Air Force organization.

1.2. Enterprise Data Management (EDM). EDM is the integrated discipline for structuring, describing, ensuring common understanding, and governing of data across organizational and technological boundaries to improve efficiency, promote transparency, and enable operational insights. To leverage data as a strategic asset, the Department of the Air Force will adopt EDM best practices. **(T-0)**. Outcomes of EDM will lead to improved data quality and assurance, information sharing for planning and conducting air, space, and cyberspace mission operations within the Department of the Air Force. Business practices will evolve by optimizing data reuse to minimize data redundancy. EDM will be used in the Department of the Air Force to enhance data sharing and enable data to be visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS). **(T-0)**. Effective EDM will result in decision superiority by fielding accurate, readily available data for use to operationalize and enable stakeholders at all levels to make data-driven decisions.

1.2.1. Data Visibility and Accessibility. Department of the Air Force data will be visible and accessible to Department of the Air Force entities except where constrained by law, regulation, security classification, guidance, or policy. **(T-0)**. Data constraints may include but are not limited to personally-identifiable information (PII) protected pursuant to 5 USC § 552a (also known as the Privacy Act of 1974); individually identifiable protected health information (PHI) according to Section 264 of Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996*; information exempted from mandatory public disclosure in accordance with 5 USC § 552 (Freedom of Information Act (FOIA)); information within systems covered under attorney-client privilege or attorney work product; information restricted from release due to security classification; and information controls on secondary release and dissemination of technical documents and data marked with the distribution statements required by DoDI 5230.24, *Distribution Statements on Technical Documents*.

1.2.1.1. Data will be visible by creating and associating metadata (“tagging”), including discovery metadata, for each asset. **(T-0)**. Metadata standards will comply with applicable national and international consensus standards for metadata exchange. **(T-0)**. These metadata standards, will be in accordance with DoDI 8320.02. **(T-0)**.

1.2.1.2. At minimum, data will be identified and tagged with its security metadata, to include the classification determination, markings, disclosure, and handling rules in order to support access control in accordance with DoDI 8320.07. **(T-0)**.

1.2.1.3. All instances of PII and PHI in the datasets will be identified and tagged. **(T-0)**.

1.2.1.4. All information required for records management (Privacy Act information, essential records indicator, FOIA Exempt Indicator, storage and archive information,

preservation information, tracking information, disposition information including date to dispose of, etc.) will be identified and tagged in accordance with AFI 33-322. (T-0).

1.2.2. Data Sharing. Department of the Air Force EDM will incorporate guidelines for ensuring data is stored and shared in accordance with Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyberspace Operations*, Air Force Manual (AFMAN) 33-396, *Knowledge Management*, and their implementing policies and procedures, as well as pursuant to 44 U.S.C § 3504. (T-0).

1.2.2.1. Intra-Service Data Sharing.

1.2.2.1.1. Data within the Department of the Air Force enterprise will be visible and accessible, and therefore does not require a data sharing agreement. (T-0).

1.2.2.1.2. Data not exempt under law, regulation, security classification, guidance, or policy will be shared within the Department of the Air Force unless an exception is approved by the SAF/CO. (T-0). Exceptions will be limited and approved only when an adverse effect on the Department of the Air Force mission will be significantly increased if the exception is not granted. (T-0). Approval authority will not be delegated. (T-1).

1.2.2.2. Inter-Service or Inter-Agency Data Sharing. All data shared between the Department of the Air Force and one or more DoD Components, non-DoD federal agencies, or federally-recognized Indian tribe will be executed as a Memorandum of Agreement, in accordance with AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*. (T-0). Data collected or created in pursuit of independent research and development will also be managed in accordance with DoDI 3204.01, *DOD Policy for Oversight of Independent Research and Development (IR&D)*. (T-0).

1.2.2.3. All Other Data Sharing. All other data sharing not covered by Paragraphs 1.2.2.1 and 1.2.2.2, to include sharing with one or more State or local governmental agencies, industries, or academia, will maximize benefit to the Department of the Air Force mission and comply with all applicable laws, regulations, and policy. (T-0). Contact the servicing judge advocate for guidance on applicable law, regulation, and policy and prior to entering into a data sharing agreement. (T-1).

1.2.2.4. Data Sharing Standards.

1.2.2.4.1. Metadata. Metadata is used to share data by providing users with the ability to easily identify applicable information from outside their respective purviews. Using metadata also enables assessments of data sharing and usage throughout the organization. SAF/CO will drive data sharing and reuse through cataloging and exposure of robust metadata, data stewardship, and dynamic processes for ensuring common data understanding. (T-0).

1.2.2.4.2. Data Sharing Agreements. The capabilities created from sharing data across the Department of the Air Force will be assessed and documented using time-evolving measurements. (T-0). Data sharing agreements detail the processes, procedures, and sharing of data between organizations. At minimum, all Department of the Air Force data sharing agreements will document, in writing, the following (T-0):

- 1.2.2.4.2.1. The parties entering into agreement (organization names and contact information for primary and alternate points of contact); **(T-0)**
- 1.2.2.4.2.2. The legal authority leveraged and the reasons for entering into the data exchange to make the data exchange permissible; **(T-0)**
- 1.2.2.4.2.3. The responsibilities and obligations of the agreement parties, including addressing third party rights and responsibilities; **(T-0)**
- 1.2.2.4.2.4. The data and supplemental information must be requested; **(T-0)**
- 1.2.2.4.2.5. The method for data sharing must include details about the supplying and receiving system or data platform; **(T-0)**
- 1.2.2.4.2.6. The frequency at which data will exchange, update, or backup; **(T-0)**
- 1.2.2.4.2.7. The data supplier's access to information and decision rights following any exchange; **(T-0)**
- 1.2.2.4.2.8. The security and access control requirements for data exchange and receipt, including how access control will be audited for the record; **(T-0)**
- 1.2.2.4.2.9. Timely reporting of incidents affecting data covered by the Agreement; **(T-0)**
- 1.2.2.4.2.10. The resource impacts for implementing data sharing; **(T-0)**
- 1.2.2.4.2.11. The methods for mitigating risk and resolving disputes; **(T-0)** and,
- 1.2.2.4.2.12. The terms for agreement termination or transference and any notice period will be required. **(T-0)**.

1.3. Data Capabilities. Data standards facilitate interoperability and are necessary for data to be shareable and discoverable across the enterprise. To increase Airmen and Guardian access to the right combinations of technologies to better utilize data as a part of their mission, the following must be achieved:

1.3.1. Data Architecture Standards. The Department of the Air Force Data Services Reference Architecture (DSRA) provides clear guidance for the design, development, implementation, and use of United States Air Force and United States Space Force data platforms and architectures. The DSRA is available at <https://org2.eis.af.mil/sites/13007/Pages/policies.aspx>. In accordance with DAFI 17-140, *Architecting*, data architectures must be developed to provide a common data-sharing technical framework between mission and EDM, and support enterprise-wide data availability. **(T-0)**.

1.3.2. Data Governance Standards. Enterprise data governance is established to orchestrate people, processes, structures, and technology that enable an organization to leverage data as an enterprise asset. It includes policies, practices, principles, and the assignment of roles and responsibilities for data management program participants. The data management program and governance bodies are developed and implemented to ensure consistency of data across the Department of the Air Force. Data governance and data stewardship disciplines facilitate the delivery of the right data to the right user at right place at the right time.

1.3.2.1. Data governance bodies support data assurance and interoperability. These bodies also function to inform decisions to shape a more data-driven Department of the Air Force

culture based on feedback, and facilitate a collaborative Department of the Air Force data environment through consistent communication.

1.3.2.2. Data stewardship fosters an environment suitable to optimal mission performance by promoting accountability for data as an enterprise asset and enabling efficient collaboration among necessary stakeholders. Effective data stewardship is fundamental to successful data governance and will ensure data is VAULTIS. See [Chapter 3](#).

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force Chief Data Officer (SAF/CO). In accordance with Headquarters Air Force Mission Directive (HAFMD) 1-5, *Air Force Chief Data Officer*:

2.1.1. Advocates and promotes the vision and goals for EDM, publicly available Department of the Air Force data, and data capabilities.

2.1.2. Surveys the enterprise to seek enterprise licenses and contracts for acquiring data resources in coordination with the Assistant Secretary of the Air Force for Acquisition, Technology & Logistics (SAF/AQ) and Deputy Chief Information Officer (SAF/CN).

2.1.3. Directs data integration through identification of metadata standards and use of application programming interfaces.

2.1.4. Establishes Department of the Air Force data governance forums to build community collaboration, to gather input, enforce sound data governance policy and processes, and make strategic decisions that impact the capabilities of Department of the Air Force data.

2.1.5. Directs Functional, United States Air Force major commands (MAJCOMs), and United States Space Force field commands, and direct reporting units (DRUs) to appoint a data officer for their organization.

2.1.6. Identifies and communicates enterprise data standards which support interoperability in accordance with DoDI 8320.02.

2.1.7. Advocates and sponsors initiatives to drive change for a data management culture throughout the Department of the Air Force.

2.1.8. Coordinates with the Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6) and Director of Intelligence, Surveillance and Reconnaissance (SF/S2) on all data policy, guidance, standards and architecture to ensure compliance with the directives and requirements of the Intelligence Community.

2.1.9. Ensures all SAF/CO EDM systems are designed and built (from the inception) to facilitate the tracking of records management information, including PII and PHI.

2.2. Deputy Chief Information Officer (SAF/CN).

2.2.1. Collaborates with SAF/CO to improve data related activities and standards pertaining to data architecture, data management, data quality, data sharing, and information assurance across the DAF.

2.2.2. Accounts for Department of the Air Force data requirements in planning infrastructure upgrades.

2.2.3. Provides guidance and policies for securing data.

2.2.4. Provides guidance and policies for records management of data and other electronic records.

2.2.5. Works with the Defense Information Systems Agency to develop an investment strategy for enterprise information technology platforms, networks, systems, and architecture assuring ability to facilitate EDM.

2.3. Deputy under Secretary of the Air Force, Management (SAF/MG).

2.3.1. Supports investment strategy on enterprise data tools.

2.3.2. Partners with SAF/CO to capture program evaluation best practices, evaluate data capacity-building and data sharing measurements for performance management, and define goals to improve data maturity.

2.4. General Counsel of the Department of the Air Force (SAF/GC). Advises on legal matters related to data governance, data sharing and usage activities, and EDM.

2.5. Department of the Air Force, Office of the Air Force Judge Advocate General (DAF/JA). Advises on legal matters related to data governance, data sharing and usage activities, and EDM. Provides functional oversight to judge advocates advising MAJCOM, Field Command, DRU, and subordinate units.

2.6. The Administrative Assistant to the Secretary of the Air Force (SAF/AA). Advises and supports SAF/CO on information security concerns related to compilation of information.

2.7. Assistant Secretary of the Air Force for Acquisition, Technology & Logistics (SAF/AQ).

2.7.1. Establishes structure and processes to support SAF/CO in satisfying acquisition oversight, cost efficiency, innovative contracting, strategic sourcing methods, and information security for the acquisition of data resources.

2.7.2. Coordinates with SAF/CO to develop standard contractual language to support to support VAULTIS data and data management sharing activity.

2.7.3. Ensures data management and sharing requirements are incorporated into program planning and acquisition strategy documentation.

2.8. Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations (AF/A2/6). .

2.8.1. Coordinates with SAF/CO and SF/S2 on Department of the Air Force data policy, standards, and architecture to ensure compliance with the directives and requirements of the DoD and Intelligence Community in accordance with HAFMD 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance and Reconnaissance* and AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*.

2.8.2. Reviews data-relevant capability, system and service's plans, programs and budgets to ensure compliance with Intelligence Community (IC) policy guidance to enhance Department of the Air Force access to IC data and enterprise services.

2.9. Deputy Chief of Staff, Strategy, Integration, and Requirements (AF/A5).

2.9.1. Coordinates with SAF/CO to ensure data architecture policy development aligns with future force design across the Department of the Air Force.

2.9.2. Provides guidance for capability development and resourcing priorities to ensure federated data platforms are fielded in an integrated Department of the Air Force, as outlined in the DSRA.

2.10. Functional, MAJCOM, Field Command, and DRU Data Officers.

2.10.1. Participate in the Department of the Air Force data governance fora as appointed by their organization to represent their organization's interest in EDM and data sharing.

2.10.2. Act as liaison for their respective organizations to integrate the operation and management of data sharing and EDM in support of integrated data capabilities and informed decision-making.

2.10.3. Communicate plans and execute data management with financial, manpower, and other resources to make data VAULTIS.

2.10.4. Facilitate execution of data sharing agreements before data is shared outside the Department of the Air Force.

2.10.5. Inform SAF/CO on data-related matters across the enterprise through data forums to eliminate duplicative efforts and enable enterprise wide capabilities.

2.10.6. Collaborate regularly with other data officers across the enterprise through governance forums to include the Department of the Air Force Data Board.

2.10.7. Ensure data collection and tagging in accordance with Department of Air Force data policies and implementation guidance.

2.11. Functional, MAJCOM, Field Command, and DRU Data Stewards. Control and provide oversight of their specifically assigned Department of the Air Force data assets to supply its users with high-quality and easily accessible data in a consistent manner.

Chapter 3

DATA STEWARDSHIP

3.1. Scope. Data Stewardship is critical to making data visible and accessible across the enterprise. In order to drive advanced capabilities, including artificial intelligence, machine learning, and next-generation decision dashboards, data will need to be available as an enterprise service. **(T-0)**. Every Airman and Guardian is a data steward. Stewardship responsibilities differ between the strategic, operational and tactical levels. Data will be aligned to mission area domains at the strategic level, then further divided into categories at lower level tiers. **(T-0)**. Lead organizations, and the Department of the Air Force data governance bodies as required, and will be identified to help de-conflict between functional and MAJCOM leads for particular data categories. **(T-0)**.

3.2. Data Stewards.

- 3.2.1. Act with authority and accountability for management of assigned data within their purview. **(T-1)**.
- 3.2.2. Control data and resolve issues for data. **(T-1)**.
- 3.2.3. Represent their respective community in data governance bodies. **(T-1)**.
- 3.2.4. Provide subject matter expertise in the context of mission execution to catalog data under their area of responsibility. **(T-1)**.
- 3.2.5. Employ use of data architectures which support enterprise-wide data availability and adhere to the Department of the Air Force DSRA. **(T-1)**.
- 3.2.6. Identify and tag data to facilitate the tracking of PII, PHI, and security classification details in the datasets hosted, handled, or used. **(T-0)**.
- 3.2.7. Identify and tag all data required for records management (Privacy Act information, essential records indicator, FOIA exemptions, storage and archive information, preservation information, tracking information, disposition information including date to dispose of, etc.) in accordance with AFI 33-322 for the datasets hosted, handled, or used. **(T-0)**.
- 3.2.8. Publish and link data assets and associated business metadata to shared locations, application program interfaces, or other web services to make data visible and accessible. **(T-1)**.
- 3.2.9. Document rules, policies, and standards for use of data within their area of responsibility. **(T-1)**.
- 3.2.10. Provide subject matter expertise to assist SAF/CO with drafting data definitions, and impact analyses, as well as establishing data quality standards, and assigning data sensitivity levels. **(T-0)**.
- 3.2.11. Collaborate with other data stewards to ensure common understanding for data. **(T-0)**.
- 3.2.12. Recommend authorization requirements and services for role-based access control. **(T-0)**.
- 3.2.13. Publish data quality and security reports. **(T-0)**.

EILEEN M. VIDRINE, SES
Chief Data Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 90-70, *Enterprise Data Management*, 13 February 2020

Public Law 115-435, *Foundations for Evidence-Based Policymaking Act of 2018*, 14 January 2019

44 USC § 3502

44 USC § 3504(b)

44 USC § 3506(b)

44 USC § 3506(d)

44 USC § 3520

DoDD 8000.01, *Management of The Department of Defense Information Enterprise (DoD IE)*, 17 March 2016

DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*, 5 August 2013

DoDI 8320.07, *Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense*, 3 August 2015

DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, January 29, 2019

DAFPD 17-2, *Cyberspace Operations*, 27 October 2020

DAFI 17-140, *Architecting*, 29 June 2018

AFMAN 33-396, *Knowledge Management*, 12 August 2019

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

Privacy Act (5 USC § 552a)

PL 104-191, *Health Insurance Portability and Accountability Act of 1996*

Freedom of Information Act (5 USC § 552)

DoDI 5230.24, *Distribution Statements on Technical Documents*, 23 August 2012

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*, 18 October 2013

DoDI 3204.01, *DoD Policy for Oversight of Independent Research and Development (IR&D)*, 20 August 2014

HAFMD 1-5, *Air Force Chief Data Officer*, 13 September 2019

HAFMD 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance and Reconnaissance*, 18 September 2015

AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*, 11 July 2019

Executive Office of the President, *The Common Approach to Federal Enterprise Architecture*, 2 May 2012

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5123.01, *Charter Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)*, 31 August 2018

Data Management Association, *Data Management Body of Knowledge* (2nd Edition), July 2017

DoDI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*, 21 May 2014

DoDD 8115.01, *Information Technology Portfolio Management*, 10 October 2005

DoD Chief Information Officer Memorandum, *Department of Defense Data Management Lexicon*, 15 June 2020

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF/A2/6—Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations

AF/A5—Air Force Strategy, Integration and Requirements

DAF/JA—Department of the Air Force, Office of the Judge Advocate General

AFPD—Air Force Policy Directive

AFMAN—Air Force Manual

CDOC—Chief Data Officer Council

DAFI—Department of the Air Force Instruction

DAFPD—Department of the Air Force Policy Directive

DAMA DMBOK—Data Management Association – Data Management Body of Knowledge

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DRU—Direct Reporting Units

DSRA—Department of the Air Force Data Services Reference Architecture

EDM—Enterprise Data Management

FOIA—Freedom of Information Act

HAFMD—Headquarters Air Force Mission Directive

IC—Intelligence Community

IT—Information Technology

MAJCOM—Major Commands

OPEN—Open, Public, Electronic, Necessary

PII—Personally Identifiable Information

PHI—Protected Health Information

SAF/AA—The Administrative Assistant to the Secretary of the Air Force

SAF/AQ—Assistant Secretary of the Air Force for Acquisition

SAF/CN—Deputy Chief Information Officer

SAF/CO—Chief Data Officer

SAF/GC—General Counsel and the Department of the Air Force

SAF/MG—Deputy Under Secretary, Management

USC—United States Code

VAULTIS—visible, accessible, understandable, linked, trustworthy, interoperable, and secure

Terms

Accessible—Data and services can be accessed via the Global Information Grid by users and applications in the enterprise. Data and services made available to any user of applications, except where limited by law, policy, security classification, or operational necessity (Ref: DoD Information Enterprise Architecture Version 3.0; AFI 17-140).

Architecture—A systematic approach that organizes and guides design, analysis, planning, and documentation activities. (*The Common Approach to Federal Enterprise Architecture*, May 2012)

Capability—The ability to complete a task or execute a course of action under specified conditions and level of performance (CJCSI 5123.01), and physical representation of data.

Data—Recorded information, regardless of form or the media on which it is recorded (44 USC § 3502)

Data Architecture—Defines the blueprint for managing data assets by aligning with organizational strategy to establish strategic data requirements and designs to meet the requirements (Ref: Data Management Association – Data Management Body of Knowledge (DAMA DMBOK) 2nd Edition). Includes abstraction, conceptual, logical, and physical models; high-level data concepts and their relationships; data requirements; data structures; and metadata models. (CJCSI 5123.01)

Data Asset—A collection of data elements or data sets that may be grouped together (44 USC § 3502).

Data Governance—The exercise of authority, control, and shared decision making (planning, monitoring, and enforcement over the management of data assets. (DAMA DMBOK 2nd Edition)

Data Officer—An empowered designee selected by the directorate that will facilitate the sharing of Department of the Air Force data across the enterprise.

Data Standards—A documented agreement and specification by an authoritative body on a definition, representation, or format of data, metadata, or exchange protocol that is used to improve data understanding and data interoperability. A data standard requires a narrative specification and may include complementary data engineering resources to guide IT system development and testing conformance. Widespread adoption of a well-designed data standard can reduce ambiguity and the necessity for mediation, while promoting efficiency and transparency of mediation where required (Ref: DoDI 8320.07).

Data Steward—Data stewards manage data assets on behalf of others and in the best interest of the organization. Data stewards represent the interest of all stakeholders and must take an enterprise perspective to ensure enterprise data is of high quality and can be used effectively. Based on the stewardship framework, data stewards are differentiated by their place within the organization and by the focus of their work. (DAMA DMBOK 2nd edition)

Enterprise—An area of common activity and goals within an organization or between several organizations, where information and other resources are exchanged. (*The Common Approach to Federal Enterprise Architecture*, May 2012)

Enterprise 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 data professionals following established disciplines and functions. (DoD Office of the Chief Information Officer Memorandum, *DoD Data Management Lexicon*, dated June 15, 2020, as derived from DAMA DMBOK 2nd Edition, 2017. IC Chief Data Officer Council (CDOC) Approved: Jun 2018)

Information—The meaning assigned to data by a known rule or set of rules. Generally, understanding concerning any objects such as facts, events, things, processes, or ideas, including concepts that, within a certain context and timeframe, have a particular meaning. The interpretation of data based on its context, including the: a) The business or mission meaning of data elements and related terms; b) The format in which the data is presented; c) The timeframe represented by the data; and, d) The relevance of the data to a given usage. (DoD Office of the Chief Information Officer Memorandum, *DoD Data Management Lexicon*, dated June 15, 2020, as derived from DAMA Dictionary of Data Management, 2nd Edition, 2017 and Hargrave's Communication Dictionary. IC CDOC Approved: Apr 2018)

Interoperability—The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (DoDI 8330.01).

Linked—Two or more items that are suggestively related.

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 USC § 3502).

Mission Areas—A defined area of responsibility with functions and processes that contribute to mission accomplishment. (Definitions) The DoD Mission areas are the Warfighting Mission Area (WMA), Business Mission Area (BMA), DoD portion of Intelligence Mission Area (DIMA), and Enterprise Information Environment (EIE) Mission Area (EIEMA) (Ref: DoDD 8115.01)

Trusted—Users and applications can determine and assess the suitability of the source because the pedigree, security level, and access control level of each data asset or service is known and available (DoD Information Enterprise Architecture Version 2.0).

Understandable—Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs (DoD Information Enterprise Architecture Version 2.0).

Visible—The property of being discoverable. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or “made visible” by providing metadata, which describes the asset (DoD Information Enterprise Architecture Version 2.0).