BY ORDER OF THE COMMANDER SPACE TRAINING AND READINESS COMMAND

SPACE TRAINING AND READINESS COMMAND INSTRUCTION 90-700

12 AUGUST 2025

Special Management

DATA MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ STARCOM/CDAO

Certified by: HQ STARCOM/CDAO

Pages: 24

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, Definitions, 3504(b), Authority and functions of Director, 3506(b) and (d), Federal agency responsibilities, and 3520, Chief Data Officers; 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 Space Training and Readiness Instruction (STARCOMI) applies to STARCOM individuals at all levels who prepare, manage, review, disseminate or use United States Space Force (USSF) data, including all civilian employees and uniformed members of STARCOM and those with a binding agreement or contractual obligation to abide by the terms of STARCOM issuances. It does not apply to the Air National Guard, Air Force Reserve Command, or the United States Air Force. This STARCOMI identifies Data Management guidelines for leveraging data as a strategic asset to meet USSF mission requirements. It also establishes the STARCOM guidance to achieve Field Command (FLDCOM)-wide data visibility and accessibility, and addresses standards for data sharing under the direction of the Chief Data and Artificial Intelligence Officer (STARCOM/CDAO). 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*. 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 DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. Submit requests for waivers through the chain of command to the publication OPR for non-tiered compliance items.

Chapter 1

DATA MANAGEMENT

1.1. Background. Data is a strategic asset that must be properly managed to be a force multiplier to improve United States Space Force (USSF) and Space Training and Readiness Command (STARCOM) mission effectiveness, readiness, lethality, and fiscal responsibility. Data and the information derived from it belong to the Department of Defense (DoD). Department of the Air Force (DAF) generated data is not owned by the data producer, a particular application, and/or DAF organization. Data producers collect, share, and integrate data that is authenticated, validated, and produced to support business and mission activities.

1.2. Data Management (DM). DM is the integrated discipline for structuring, describing, ensuring common understanding of, and governing data across organizational and technological boundaries to improve efficiency, promote transparency, and enable operational insights. To leverage data as a strategic asset, STARCOM will adopt DM best practices. Outcomes of DM will lead to improved data quality, information sharing for planning, and executing space missions assigned to STARCOM. Business practices will evolve by optimizing data reuse to minimize data redundancy. DM will be used in STARCOM to enhance data sharing and enable data to be Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure (VAULTIS) as prescribed in the Department of Defense (DoD) Data Strategy. Effective DM 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.

1.2.1.1. Data will be visible and accessible to DAF entities except where constrained by law, regulation, security classification, guidance, or policy. Data constraints may include but are not limited to Personally Identifiable Information (PII) protected pursuant to 5 USC § 552a, Records maintained on individuals (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 Department of Defense Instruction (DODI) 5230.24, *Distribution Statements on DoD Technical Information.*

1.2.1.2. Data will be visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. Metadata standards will be in accordance with DoDI 8320.02.

1.2.1.3. At minimum, data will be identified and tagged with its security metadata, to include the classification determination, markings, disclosure, and handling rules to support access control in accordance with DoDI 8320.07.

1.2.1.4. All instances of PII and PHI in the data sources will be identified and tagged.

1.2.1.5. 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.

1.2.2. Data Sharing and Storage.

1.2.2.1. STARCOM DM ensures data is stored and shared in accordance with Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations;* DAFI 90-7001, *Enterprise Data Sharing & Data Stewardship*; Air Force Manual (AFMAN) 33-396, *Knowledge Management;* as well as pursuant to 44 U.S.C § 3504, *Authority and functions of Director,* paragraph (b)(B). Approved data storage includes DAF Microsoft 365 hosted applications within the DAF cloud, plus DoD and DAF data lakes (examples provided below, not all-inclusive).

1.2.2.1.1. Advanced Analytics (ADVANA). Directed as the DoD data catalog, authoritative DAF data sources must federate to ADVANA. ADVANA provides authoritative financial data sources and a centralized environment for DoD users to access and analyze data from various systems, enabling data-driven decision-making across the organization. ADVANA aims to make data more accessible, understandable, and actionable, ultimately improving decision-making and efficiency within the DoD.

1.2.2.1.2. ENVISION. ENVISION data platform is a secure, cloud-based platform used by the DAF for data manipulation, visualization, and decision-making. It helps integrate data feeds across the enterprise and commercial sources to support operations, readiness, and training. ENVISION integrates data across the DAF, DoD, and civilian agencies, provides a data catalog and analytic environment.

1.2.2.1.3. USSF Unified Data Library (UDL). The UDL is a cloud-based data repository that ingests and consolidates data from government and commercial sensors in support of USSF missions.

1.2.2.1.4. Basing and Logistics Analytics Data Environment (BLADE). BLADE is an Air Force- specific application that leverages the ADVANA platform, focused on consolidating and analyzing basing and logistics data sources to improve decision-making and operational efficiency.

1.2.2.1.5. Enterprise Logging Ingest and Cyber Situational Awareness Refinery (ELISCAR). ELISCAR is designed to support Cyber Warfare Defensive Cyber Operations (DCO) missions. It is based on the Defense Information Systems Agency (DISA) Big Data Platform. Software ingests and stores large data sources from internal and external sources, running analytics to rapidly detect Indicators of Compromise (IOC). ELICSAR provides the tools for Cyber Warfare to make timely data driven decisions to defend the Air Force Network (AFNET).

1.2.2.1.6. Visible, Accessible, Linked and Trusted (VAULT). The VAULT Platform is designed to provide secure cyber, cloud-based tools to connect, find, share and learn from DAF data to improve readiness and mission success. The VAULT Platform has a set of tools to support a full lifecycle of data exploitation activities. It provides data ingest, storage, metadata management, data sorting, cleaning, and experimentation, and visualize analytics results. Data sources and applications have access controls that are

group and role based. The visualization service supports multiple user groups leveraging a common application platform.

1.2.3. Intra-Service Data Sharing.

1.2.3.1. Visible and accessible data does not require a data sharing agreement.

1.2.3.2. Data not exempt under law, regulation, security classification, guidance, or policy will be shared unless an exception is approved by the Air Force Chief Data Officer (SAF/CO). Exceptions will be limited and approved only when an adverse effect on the DAF mission will be significantly increased if the exception is not granted. Approval authority will not be delegated.

1.2.4. Inter-Service or Inter-Agency Data Sharing.

1.2.4.1. All data shared between the DAF and one or more DoD Components, non-DoD federal agencies, or federally recognized Indian tribe will be exchanged and/or managed as prescribed by a Memorandum of Agreement (MOA), in accordance with AFI 25-201, *Intra-Service, Intra- Agency, and Inter-Agency Support Agreements Procedures.* 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).*

1.2.5. Other Data Sharing.

1.2.5.1. All other data sharing not covered by paragraphs **1.2.2, 1.2.3,** and **1.2.4**, to include sharing with one or more State or local governmental agencies, industries, or academia, must comply with applicable laws, regulations, and policy. STARCOM members must contact the servicing judge advocate for guidance on applicable laws, regulations, and policies prior to entering into a data sharing agreement.

1.2.6. Metadata Tagging.

1.2.6.1. 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. STARCOM will drive data sharing and reuse through cataloging and exposure of robust metadata, data stewardship, and dynamic processes for ensuring common data understanding.

1.2.7. Data Sharing Agreements.

1.2.7.1. Data sharing agreements detail the processes, procedures, and sharing of data between organizations (reference **Attachment 4** for additional information*)*. Per DAFI 90-7001, paragraph 1.2.2.4.2, at minimum all data sharing agreements will document the following:

1.2.7.1.1. List the parties entering into agreement (organization names and contact information for primary and alternate points of contact).

1.2.7.1.2. Identify the legal authority leveraged and the reasons for entering into the data exchange to make the data exchange permissible.

1.2.7.1.3. Outline the responsibilities and obligations of the agreement parties, including addressing third- party rights and responsibilities.

1.2.7.1.4. The data and supplemental information must be requested.

1.2.7.1.5. The method for data sharing must include details about the supplying and receiving system or data platform.

1.2.7.1.6. Frequency at which data will exchange, update, or backup.

1.2.7.1.7. Data supplier's access to information and decision rights following any exchange.

1.2.7.1.8. Security and access control requirements for data exchange and receipt, including how access control will be audited for the record.

1.2.7.1.9. Timely reporting of incidents affecting data covered by the Agreement.

1.2.7.1.10. Resource impacts for implementing data sharing.

1.2.7.1.11. Methods for mitigating risk and resolving disputes.

1.2.7.1.12. Terms for terminating the agreement, or transference, and any notice period will be required.

1.2.7.1.13. Data Sharing Agreements will be managed by and reside with the Chief of Staff office.

1.2.8. Data Architectures.

1.2.8.1. Data standards facilitate interoperability and are necessary for data to be shareable and discoverable across the enterprise. To increase access to the right combinations of technologies to better utilize data as a part of their mission, organizations must utilize the DAF Data Services Reference Architecture (DSRA). DSRA provides clear guidance for the design, development, implementation, and use of DAF data platforms and architectures. The SAF/CO DSRA is available at: **https://www.af.mil/Portals/1/documents/2019%20SAF%20story%20attachments/Tab%203%20SAF_CO_DSRA_Formatted.pdf?ver=2019-05-08-151010-237**. In accordance with AFI 17-140, *Architecting;* data architectures must be developed to provide a common data-sharing technical framework between mission and DM, and support enterprise-wide data availability.

1.2.9. Data Governance.

1.2.9.1. 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 participants. Data management governance bodies (Working Groups, Boards, and Councils) are developed and implemented to ensure consistency of data management activities across the DAF enterprise. Data governance and data stewardship disciplines facilitate the delivery of the right data to the right user at right place at the right time.

1.2.9.2. Data governance bodies (Working Groups, Boards, and Councils) support data assurance and interoperability. These bodies also function to inform decisions to shape a more data-driven culture based on feedback and facilitate a collaborative data environment through consistent communication.

1.2.9.3. Data Stewards fosters an environment suitable for optimal mission performance by promoting accountability for data as an enterprise asset and enabling efficient collaboration among necessary stakeholders. Data Stewards for STARCOM are appointed and across the command at the Colonel or equivalent level for the Headquarters staff, at the Materiel Lead level for the Operational Test and Training Integrated Program Office (OTTI IPO), and at the Commander level or equivalent for the Deltas (reference **Attachment 3** for the STARCOM Data Steward Appointment Letter Template).

1.2.10. Data Ethics.

1.2.10.1. The ethical use of data will be at the forefront of all plans and actions for how data is collected, used, and shared. As the Secretary of Defense stated in his guidance on Artificial Intelligence (AI) Ethics on February 21, 2020, “Although technology changes, the Department's commitment to the Constitution, the Law of War, and the highest standards of ethical behavior does not.” Whether for AI or advanced analytics, ethical principles regarding the responsible use of data remain important. Component Data Stewards will be responsible for promoting a culture of ethical data use supported by oversight mechanisms to identify and promote best practices.

Chapter 2

DATA COLLECTION

2.1. Data Collection. Data collection is the obtaining, causing to be obtained, soliciting, or requiring data to be disclosed by an organization, third parties or the public. Formal data collection for mission and business authoritative data sources may require the completion of a Data Sharing Agreement, Data Collection Request, and/or Data Access Request form. Routine STARCOM business data sharing and collection activities normally will not require these forms.

2.2. Mission-Authorized Collection.

2.2.1. Data collection must be directly tied to approved STARCOM mission taskings, functions, training objectives, Test and Evaluation (T&E) activities, and/or Artificial Intelligence/Machine Learning (AI/ML) model development. The DAF has an obligation, and shall continue in the conduct of its activities, to protect fully the legal rights of all United States (US) persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law. Data collection concerning individuals or legal entities (especially US personnel) must also comply with DODD 5148.13, *Intelligence Oversight*; Department of Defense Manual (DODM) 5240.01, *Procedures Governing the Conduct of the DoD Intelligence Activities*; and DAFI 14-404, *Intelligence Oversight*.

2.2.2. Data source collection requests (DCRs) or data access requests are normally electronic forms that are included as part of a platform's data catalog or library as a method to request data collection or access from the data producer and/or provider for a set period of time.

2.3. Minimum Necessary and Quality-Driven Collection.

2.3.1. Only the specific data required to achieve AI model accuracy shall be collected. This will save resources in terms of data cleaning, data storage and legal guidance.

2.3.2. Data used for AI model training must be relevant to the operational or training domain, be free of bias to the extent feasible, and documented with provenance metadata and usage limitations.

2.4. Metadata and Cataloging.

2.4.1. Authoritative data sources must federate to or be registered in an approved DAF Data catalog. Work with the STARCOM Command Data and Artificial Intelligence (CDAO) office to determine the appropriate location for your data to be registered. The catalog relies on metadata to describe data assets, enabling users to search, understand, and utilize the data. The DoD Chief Data Officer (CDO) has established minimum metadata requirements for data sets within the Federated Data Catalog in ADVANA. For information regarding ADVANA minimum metadata catalog requirements reference, *Memorandum for DoD Component Chief Data Officers,* Federated Data Catalog – Minimum Metadata Requirements, 2021.

2.4.2. The data products/outputs generated from testing, training, and evaluation models (to include AI models) must be labeled to ensure versioning history.

2.5. Ethical AI and Consent Requirements.

2.5.1. Personal or human subject data collection, use, storage, and retention must comply with DoD I3216.02, *Protection of Human Subjects and Adherence to Ethical Standards in DAF-*

Conducted and-Supported Research. Also, data concerning individuals or legal entities (especially US persons) must also comply with DODD 5148.13, *Intelligence Oversight*; Department of Defense Manual (DODM) 5240.01, *Procedures Governing the Conduct of the DoD Intelligence Activities*; and DAFI 14-404. Furthermore, in accordance with AI Ethical Principles, a review by the STARCOM Judge Advocate General's (JAG) office is required for STARCOM developed AI. The JAG Corps' legal and ethical obligations align with the DoD AI Ethical Principles in ensuring AI systems are legally compliant, ethically sound, accountable, and transparent.

2.5.2. Synthetic data or anonymization must be applied where real operational or training data introduces privacy, classification, or bias concerns.

Chapter 3

DATA RETENTION

3.1. Retention Periods.

3.1.1. Data shall be retained based on its operational, historical, or analytical value, as outlined in the STARCOM Data Retention Schedule:

3.1.1.1. Mission Training Data: Retained for a minimum of 7 years or until superseded by new scenarios or doctrine.

3.1.1.2. AI Training Data Sources: Retained for the life of the model plus 5 years for auditability, retraining, and revalidation purposes.

3.1.1.3. T&E Data: Retained for 7 years or as required by test certification standards.

3.1.2. Retention includes:

3.1.2.1. Raw training data

3.1.2.2. Pre-processed features

3.1.2.3. Labeling records

3.1.2.4. Training configuration files and model hyperparameters

3.2. AI Model Data Lineage. AI/ML models must be traceable to the data sources used in training, validation, and testing.

3.3. Secure Disposition.

3.3.1. Disposition must follow DoD data sanitization procedures (e.g., NIST SP 800-88 Rev. 1).

3.3.2. STARCOM must incorporate retention and deletion schedules, especially for data sources involving classified or AI-sensitive content. AI-sensitive content includes personal, confidential, or potentially harmful content if misused and/or exposed (e.g., medical records, or PII).

3.4. Suspension of Disposition. Any data subject to audit, investigation, or AI model drift analysis shall be retained until cleared by STARCOM JAG and Data Governance authorities.

Chapter 4

ROLES AND RESPONSIBILITIES

4.1. STARCOM Commander.

4.1.1. Support and request funding for a data and AI office with required personnel and capabilities to fully integrate data and AI into STARCOM workflows, processes, and capabilities.

4.1.2. Support the data office by approving data retention schedules and adjudicated data-related risks or exceptions.

4.1.3. Validate data-driven efforts by ensuring data is available to support analysis and decision making.

4.1.4. Validate the risk of not implementing AI capabilities when adjudicating AI necessity and future risk to mission.

4.2. STARCOM Command Data and Artificial Intelligence Officer (CDAO).

4.2.1. Serve the STARCOM Commander to establish, maintain, approve, and oversee data and FLDCOM DM activities.

4.2.2. Participates in and leads Data Governance Forums. Participates in the USSF Data and Artificial Intelligence Board to represent STARCOM's interest regarding data sharing, data-related matters, eliminate duplicative efforts, and enable/leverage enterprise capabilities. Collaborates regularly with other FLDCOM data officers, and lead as delegated by HQ USSF, HQ USSF data governance Working Groups. Establishes and leads the STARCOM Data Management Working Group (DMWG) and Board. Ensures STARCOM appointed Data Stewards from the Headquarters' Staff, Deltas, and T&E and Training Infrastructure Integrated Program Office (OTTI IPO) participate in the STARCOM DMWG, present data-related topics, issues, and products to be elevated and/or addressed at higher level USSF data governance Boards as needed.

4.2.3. Act as a liaison for STARCOM to integrate the operation and management of data sharing and DM in support of integrated data capabilities and informed decision-making.

4.2.4. Communicate plans and execute data management with financial, manpower, and other resources to accomplish data VAULTIS.

4.2.5. Facilitate execution of data sharing agreements before data is shared outside the DAF.

4.2.6. Ensure data collection and tagging in accordance with DAF data policies and implementation guidance.

4.2.7. Develop and implements a data dictionary, ontology, catalog, models, and architecture.

4.2.8. Ensure continuous development of a data savvy STARCOM culture. Identify data management and emerging technologies training and education opportunities. Identifies Data Stewards training and skill set requirements.

4.2.9. Lead implementation and oversight of this guidance, ensures AI training practices meet ethical and retention requirements.

4.3. HQ STARCOM Directors/Delta Commanders/OTTI IPO Director.

4.3.1. Provide support to the STARCOM Data Governance Construct. Designate Directorate data steward/s and provide subject matter experts, action officers, stakeholders, and leadership participation at the appropriate levels in support of the Data Management Working Group, Board and Council.

4.3.2. Ensure directorate data is VAULTIS.

4.3.3. Implement data policy and standards that enable the use of federated enterprise capabilities.

4.3.4. Develop and leverage directorate segment of the command data dictionary, ontology, catalog, models, and architecture.

4.3.5. Leverage enterprise data platforms for data storage and or data analytics using approved data analytic tools, sandboxes, and platforms.

4.3.6. Implement data ethics standards set by the DoD, DAF and USSF. Any local data ethical standards must be reviewed and approved by the STARCOM Judge Advocate (JA).

4.3.7. Designate subject matter experts as data steward/s and support activities with action officers, stakeholders, and leadership participation at the appropriate levels in support of the Data Management Boards.

4.3.8. Maintain authoritative data sources and enforce data tagging, retention, and secure handling.

4.4. STARCOM Financial Management (FM). Establish provisions in DoD 7000.14-R (Reference (p)) that direct adherence to the data and services guidance in this instruction, including a requirement for comptrollers to prohibit the execution of funds on programs, projects, and initiatives that do not comply with this instruction.

4.5. STARCOM Cyber Security (S4/6).

4.5.1. Provide mechanisms to ensure STARCOM data, information, and IT services under the Command Special Access Program Management Office (SAPMO) are properly registered, exposed, and available and secure.

4.5.2. Evolve, establish, manage, and make available the enterprise services and the interface standards and specifications for the sharing of data, information, and IT services to meet the needs of the STARCOM Components and their validated requirements.

4.5.3. In coordination with the STARCOM SAPMO and CDAO, adjudicate waivers and change requests submitted by STARCOM Components.

4.5.4. Ensure information technology architecture meets data requirements for latency and bandwidth requirements.

4.6. Data Stewards.

4.6.1. In accordance with DAFI 90-7001, Data Stewards will:

4.6.1.1. Participate in Data and AI Governance forums representing their organization’s interest in enterprise data management and data sharing.

4.6.1.2. Act as liaison to integrate the management of data sharing and enterprise data management in support of integrated data capabilities and informed decision-making while being the data expert.

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

4.6.1.4. Coordinate data sharing requests and agreements for data sources within their portfolio.

4.6.1.5. Inform STARCOM/CDAO of data-related matters across the enterprise to eliminate duplicative efforts and enable enterprise-wide capabilities.

4.6.1.6. Collaborate regularly with other data officers across the enterprise.

4.6.1.7. Ensure data collection and tagging is in accordance with DAF and STARCOM data policies and guidance.

4.6.1.8. Complete mandatory Data Steward training as directed by the CDAO, (e.g., Data and AI Training, and Introduction to Data Ethics via Digital University[**https://digitalu.af.mil/app/programs/starcom**]).

4.7. Test Directors and Model Developers.

4.7.1. Ensure AI-related data is versioned, annotated, and preserved per model lifecycle management policies.

4.7.2. Ensure all models are approved for government use and are built in accordance with government policy.

MATTHEW S. CANTORE, Brigadier General, USSF
Deputy Commander, Space Training and Readiness Command

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

44 USC § 3502, Definitions

44 USC § 3504, Authority and functions of Director

44 USC § 3506, Federal agency responsibilities

44 USC § 3520, Chief Data Officers

5 USC § 552, Public Information; Agency Rules, Opinions, Orders Records, and Proceedings (Freedom of Information Act)

5 USC § 552a, Records maintained on individuals (Privacy Act of 1974)

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

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

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

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

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

CJCSI 5123.01I, *Charter of the Joint Requirements Oversight Council (JROC) and the Implementation of the Joint Capabilities Integration and Development System*, 30 October 2021

DAFI 14-404, *Intelligence Oversight*, 23 January 2025

DAFI 90-7001, *Enterprise Data Sharing & Data Stewardship*, 22 April 2021

DAFPD 17-2, *Cyber Warfare Operations*, 27 October 2020

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

Director of National Intelligence, *Data Management Lexicon*, May 2024

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

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

DoDI 5230.24, *Distribution Statements on DoD Technical Information*, 10 January 2023

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

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 8330.01, *Interoperability of Information Technology, Including National Security Systems*, 27 September 2022

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

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

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

Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS), 30 October 2021

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

Acronyms

AI—Artificial Intelligence

CDAO—Command Data and Artificial Intelligence Officer

CDOC—Chief Data Officer Council

DAF—Department of the Air Force

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

DMWG—Data Management Working Group

DM—Data Management

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DSRA—Department of the Air Force Data Services Reference Architecture

FLDCOM—Field Command

FOIA—Freedom of Information Act

IT—Information Technology

ML—Machine Learning

MOA—Memorandum of Agreement

OPEN—Open, Public, Electronic, Necessary

IPO—Integrated Program Office

OTTI—Operational Test and Training Infrastructure

PII—Personally Identifiable Information

PHI—Protected Health Information

STARCOM—Space Training and Readiness Command

T&E—Test and Evaluation

USSF—United States Space Force

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

Office Symbols

OTTI/IPO—Operational Test and Training Infrastructure Integrated Program Office

SAF/CO—Air Force Chief Data Officer

STARCOM/CDAO—Command Data and Artificial Intelligence Office

STARCOM/FM—Financial Management

STARCOM/S4/6—Cyber Security

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).

Board—A panel of individuals, typically officers, enlisted personnel, or civilians, who convene to make decisions regarding specific matters. Boards are convened at the Colonel or equivalent level, Senior-leader decision making level.

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

Council—A panel of individuals, typically Executive-level officers, enlisted, or civilian personnel who convene to make decisions regarding specific matters. Councils are convened at the General Officer or equivalent level, Executive-leader decision making level.

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 5123.01I).

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

Data Catalog—A set of information describing the contents, format, and structure of a database, and the relationship between its elements; used to control access to and manipulation of the database.

Data Collection—Data collection is the obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of data or information by or for an agency. by means of identical questions posed to, or identical reporting, record keeping, or disclosure requirements imposed on persons or activities, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit (5 CFR 1320.3).

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 Life Cycle—The sequence of stages that a particular unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life.

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 Source—origin of data, such as a database, file, voice, video, imagery etc.

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 as 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 us 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).

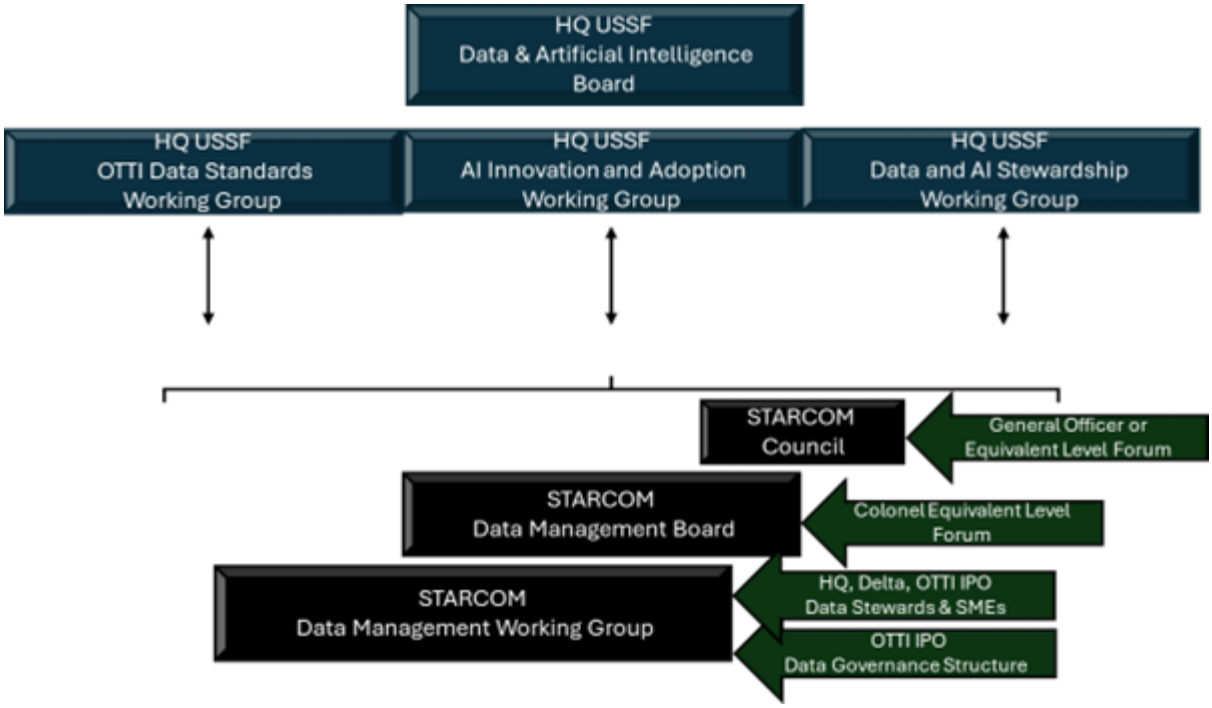
Visible—The property of being discoverable. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset (DoD Information Enterprise Architecture Version 2.0).

Working Group—an interdisciplinary collaboration of people working on a specific topic, project or problem that would be difficult to develop under a traditional organizational structure or funding mechanisms. Cross-Functional Team makeup to develop products, report issues, and generate recommendations for associated Board to enable decisions and/or direction. Team construct consists of Subject Matter Experts (SMEs) comprised of contractor support, military and civilian personnel.

Attachment 2

DATA MANAGEMENT GOVERNANCE STRUCTURE

Figure A2.1. Data Management Governance Structure.



Attachment 3

STARCOM DATA STEWARD APPOINTMENT LETTER TEMPLATE

Table A3.1. STARCOM Data Steward Appointment Letter Template.

DEPARTMENT OF THE AIR FORCE
UNITED STATES SPACE FORCE
HEADQUARTERS SPACE TRAINING AND READINESS COMMAND

XX XXX 20XX

MEMORANDUM FOR STARCOM/CDAO

FROM: (ORGANIZATION NAME HERE)

SUBJECT: Data Steward Appointment Letter

1. The following individuals from the (ORG/UNIT NAME HERE) are appointed as Data Steward (s) with delegated authority to represent organizational interests for data governance and initiatives.

Primary: Name (First, MI, Last)/Pay Grade Unit/Office Symbol

Email Address: @spaceforce.mil
Duty Phone: xxx-xxx-xxxx

Alternate: Name (First, MI, Last)/Pay Grade Unit/Office Symbol

Email Address: @spaceforce.mil
Duty Phone: xxx-xxx-xxxx

2. It is the responsibility of the Unit Director/Commander to appoint Data Stewards and keep appointment letters up to date for continuous organizational representation across the command.

3. In accordance with AFI 90-7001, Data Stewards will:

a. Participate in Data and Artificial Intelligence (AI) Governance forums to represent their organization's interest in enterprise data management and data sharing.

b. Act as liaison to integrate the operation and management of data sharing and enterprise data management in support of integrated data capabilities and informed decision-making.

c. Communicate plans and execute data management with financial, manpower, and other

resources to make data visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS).

d. Coordinate and share data from sources within their portfolio upon request.

e. Inform STARCOM/CDAO of data-related matters across the enterprise to eliminate duplicative efforts and enable enterprise-wide capabilities.

f. Collaborate regularly with other data officers across the enterprise.

g. Ensure data collection and tagging is in accordance with Department of Air Force and STARCOM data policies and guidance.

Commander/Director Signature
Unit

cc:

Attachment 4

STARCOM DATA SHARING TEMPLATE

Table A4.1. STARCOM Data Sharing Template.

Space Training and Readiness Command (STARCOM)

Data Sharing Agreement

[Date][Version Number]

[***Note: This template provides an example for a memorandum of agreement between two organizations who would like to engage in a shared confidentiality relationship in order to facilitate the exchange of data from external agencies. Organizations should feel free to adapt and customize this agreement as appropriate. Include all data sharing information points outlined in paragraph 1.2.7.1 of this Instruction***]

1. NAME OF ORGANIZATIONS ENTERING INTO AGREEMENT

Organization 1
Name of Organization Requestion Data:
Address:
Phone:

Organization 2
Name of Organization Providing Data:
Address:
Phone:

2. LEGAL AUTHORITY AND REASONS OF THE AGREEEMENT

In this section, both organizations should state in non-technical language the purpose(s) for which they are entering into the agreement. For example, data will be shared between organizations to facilitate... (add specific details here).

3. RESPONSIBILITIES AND OBLIGATIONS OF THE AGREEEMENT

In this section, both organizations should state in non-technical language their responsibilities and obligations of the agreement, including third-parties rights and responsibilities.

4. DATA TO BE SHARED AND SUPPLEMENTAL INFORMATION

In this section, capture in non-technical language the data to be shared and associated supplemental information.

5. METHOD OF DATA SHARING

In this section, capture in non-technical language the method in which data will be shared, must include details about the supplying and receiving system/s or data platform/s.

6. DATA EXCHANGE, UPDATE, AND/OR BACKUP FREQUENCY

In this section, capture in non-technical language the frequency at which data will exchanged, updated, and/or backed up.

7. DATA SUPPLIER AND DATA REQUESTOR ACTIVITIES

In this section, both organizations capture in non-technical language their access to information and decision right following any exchange.

8. DATA SECURITY

In this section, capture in non-technical language the security and access control requirements for the data exchange and receipt, including how access will be audited for the record.

9. DATA INCIDENT REPORTING

In this section, capture in non-technical language how both organizations will accomplish timely reporting of incidents affecting data covered by the agreement.

10. RESOURCE IMPACT

In this section, both organizations should state in non-technical language the resource impacts for implementing the data sharing agreement.

11. RISK MITIGATION AND DISPUTE RESOLUTION

In this section, both organizations should state in non-technical language risk and dispute mitigation methodologies.

12. AGREEMENT TERMINATION OR TRANSFER

In this section, both organizations should state in non-technical language the terms for this agreement to be terminated or transferred, and any notice period that will be required.

13. PERIOD OF AGREEEMENT

The period of agreement shall extend from _____ to _____.

14. CONFIDENTIALITY

In this section, the organizations should describe the technical and physical safeguards they will implement to protect the confidentiality of the data shared and prevent unauthorized access. This includes limiting access to individuals with a need-to-know, storing electronic data on password-protected and/or encrypted computers and tablets, etc. Organizations may also want to include a copy of the confidentiality agreement that all staff receiving data will be required to sign prior to the start of the data sharing agreement.

15. SIGNATURES

_____
Signature Block of Organization Requesting Data

_____
Signature Block of Organization Providing Data