***BY ORDER OF THE COMMANDER***
***AIR COMBAT COMMAND***

***AIR COMBAT COMMAND***
***INSTRUCTION 90-7010***

***27 MAY 2026***

***Special Management***

# *DATA AND ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: ACC/A6T CDAO

Certified by: ACC/A6

Pages: 31

---

This Air Combat Command Instruction (ACCI) provides prescriptive guidance for data and AI governance and implements Air Force Instruction (AFI) 90-7001, *Enterprise Data Sharing & Data Stewardship*, Department of War (DoW) Memorandum, *Artificial Intelligence Strategy for the Department of War (*DoW AIS Memo*),* the 2023 Department of Defense Data, Analytics, and AI Adoption Strategy (2023 DoD DAAIS): *Accelerating Decision Advantage*, Office of Management and Budget (OMB) Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the National Institute of Standards and Technology (NIST) AI 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, and is consistent with recent Executive guidance outlined in Winning the Race: America's AI Action Plan. This ACCI applies to all Air Combat Command (ACC) units, Wings, directorates, Numbered Air Forces (NAF), and Forward Operating Units, and those with a binding agreement or contractual obligation to abide by the terms of Department of the Air Force (DAF) issuances or ACC issuances. This instruction does not apply to the Air National Guard, Air Force Reserve Command, or the United States Space Force. This instruction applies to all data and/or AI in service of ACC projects, programs, and missions. This instruction does not apply to testing and evaluation of potential vendor solutions, including commercial and/or publicly available capabilities under consideration. However, data and AI governance requirements must be considered in acquisition efforts in accordance with (IAW) OMB Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government.* Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program,* and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using DAF Form

847, *Recommendation for Change of Product*; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing and unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Reference DAFMAN 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier numbers.

# Chapter 1

# DATA GOVERNANCE

**1.1. Data Governance Overview.** Data governance establishes clear policies and standards that guide data management, enhance data integrity, and ensure compliance with regulatory requirements. It focuses on the effective end-to-end lifecycle management of data, ensuring that the correct data is delivered at the speed of mission relevance. Governance establishes responsibility over data, fostering a culture of data stewardship at all levels. Data Management implements those policies, standards, guidance, and higher-level procedures within IT platforms, systems, applications, and human workflows. This structured approach not only facilitates better data utilization and sharing across ACC but also supports organizational agility and competitiveness. Some of the competencies and purposes of data governance include:

1.1.1. **Data Management and Optimization:**

1.1.1.1. Provide the principles, policies, processes, frameworks, metrics, and oversight required to effectively manage data at all levels, from creation and storage to archiving and disposal.

1.1.1.2. Cultivate data stewardship practices across various levels within ACC. Clearly define the roles and responsibilities of data stewards, ensuring they are accountable for the management of data within their purview. These roles are detailed in **paragraph 4.6** and **Attachment 2.**

1.1.1.3. Reduce data redundancy and inconsistency to minimize resource waste and enhance data integrity.

1.1.1.4. Develop stringent controls and processes to ensure data used in analytics is accurate, complete, and reliable.

1.1.2. **Organizational Management:**

1.1.2.1. Engage in organizational change management efforts that actively communicate to ACC the necessity of managing data as a strategic enterprise asset.

1.1.2.2. Facilitate cross-functional collaboration by engaging leadership, data stewards, and stakeholders at all levels to integrate data governance into decision-making processes.

1.1.3. **Data Security and Regulatory Compliance:**

1.1.3.1. Define and implement risk management processes to identify, assess, and mitigate potential risks in data handling and processing.

1.1.3.2. Integrate robust cybersecurity protocols to protect data integrity, confidentiality, and availability. This includes regular security assessments, compliance with cybersecurity standards, and implementing measures to prevent unauthorized access and data breaches.

1.1.3.3. Ensure adherence to all DoW policy and applicable law by securely managing, processing, and storing personal data, obtaining necessary consent, anonymizing data where applicable, and maintaining transparency in data usage. Consult with your servicing legal office on applicable regulations.

1.1.4. Providing foundational oversight and technical baselines to:

1.1.4.1. Align with the DoW data strategy of making data Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure (VAULTIS).

1.1.4.1.1. **Visible:** Consumers can locate the needed data.

1.1.4.1.2. **Accessible:** Consumers can retrieve the data.

1.1.4.1.3. **Understandable:** Consumers can find descriptions of data to recognize the content, context, and applicability.

1.1.4.1.4. **Linked:** Consumers can exploit complementary data elements through innate relationships.

1.1.4.1.5. **Trustworthy:** Consumers can be confident in all aspects of data for decision-making.

1.1.4.1.6. **Interoperable:** Consumers and producers have a common representation and comprehension of data.

1.1.4.1.7. **Secure:** Consumers know that data is protected from unauthorized use and manipulation.

1.1.4.2. Apply the five DoD Data Decrees detailed in the Deputy Secretary of Defense (DepSecDef) Memorandum, *Creating Data Advantage,* to reduce or eliminate barriers associated with finding, using, and sharing data tied closely to specific policies, such as those related to individual units, IT platforms, systems, applications, or workflows. Data governance and governance of IT are separate activities; however, data governance requirements will be incorporated in the procurement of new or upgraded IT to enhance future capabilities. The five DoD Data Decrees are as follows:

1.1.4.2.1. Maximize data sharing and rights for data use: all DoD data is an enterprise resource.

1.1.4.2.2. Publish data assets in the DoD federated data catalog along with common interface specifications.

1.1.4.2.3. Use automated data interfaces that are externally accessible and machine-readable; ensure interfaces use industry-standard, non-proprietary, preferably open-source, technologies, protocols, and payloads.

1.1.4.2.4. Store data in a manner that is platform and environment-agnostic, uncoupled from hardware or software dependencies.

1.1.4.2.5. Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use.

1.1.4.3. Align with HHQ data and metadata commonality standards for analytics, automation, data fusion, and artificial intelligence/machine learning (AI/ML) at scale which will reduce the complexity and time associated with developing analytics, automation, fusion, and AI/ML using heterogeneous data without a common baseline.

1.1.4.4. Enhance the ability of analysts, researchers, leaders, and warfighters to leverage mission data to gain required operational efficiencies and tactical advantages. IAW the DAF *Application Program Interface (API) Reference Architecture*, Enterprise API services

will connect end users and systems to data and software interfaces to boost accessibility, as well as standardize and increase the ease of integration with mission partners, other government entities, and industry providers to improve interoperability.

**1.2. Background.** Historically, the lack of cohesive data governance policies has led to ad hoc data management practices, resulting in inefficiencies, departmental data silos, and inconsistent data quality. These issues have hindered ACC's ability to leverage data effectively for decision-making, innovation, and achieving strategic objectives.

**1.3. Purpose.** This instruction is intended to direct and guide ACC in accelerating its data governance practices and applications to align with the DoW data strategy of making data VAULTIS, creating the foundation necessary to achieve decision advantage through AI. This instruction will:

1.3.1. Address data governance challenges for all ACC personnel, processes, structures, and technologies.

1.3.2. Ensure technical implementation of data governance is aligned with DoW and DAF standards. ACC Intelligence, Surveillance, and Reconnaissance (ISR) units must abide by ACCMAN 14-422, *Intelligence Data Governance*.

1.3.3. Identify key data roles and responsibilities and define annual reporting. Collect metrics to track data governance implementation actions, adherence to standards and policies, and the collective enterprise effects.

**1.4. Strategy and Framework.** Implementing a data governance program will require a commitment to change. The following principles are essential in a sturdy foundation for data governance.

1.4.1. **Leadership and Strategy:** Successful data governance depends on vision and committed leadership. ACC's vision and activities are informed by strategies provided by the DoW and DAF.

1.4.2. **Enterprise Driven:** Data governance is not confined to a single department; it requires enterprise-wide implementation. Therefore, the effectiveness of data governance depends on influencing data-related decisions across the entire enterprise, including IT.

1.4.3. **Shared Responsibility:** Data governance is a shared responsibility among data creators, users, stewards, and technical data management professionals.

1.4.4. **Multi-layered:** Data governance spans the entire organization to include all levels of ACC.

1.4.5. **Framework-based:** Because activities require coordination across functional areas, data governance must establish an operating framework that defines accountabilities and interactions while satisfying interoperability needs and mission goals. The governance bodies responsible for establishing the framework are detailed in **paragraph 3.3**.

1.4.6. **Technology Enabled:** Data governance relies on leveraging suitable technology to streamline and support governance activities. Selecting and implementing the right tools ensures efficient management and integrity of data across ACC.

1.4.7. **Mission Driven:** Data governance is a direct enabler of warfighting advantage. All governance activities should contribute to operational outcomes.

## Chapter 2

## AI GOVERNANCE

**2.1. AI Governance Overview.** AI governance is a comprehensive framework that enables effective and appropriate management of AI within ACC, consistent with the guiding principles and priorities laid out in recent Executive guidance, Winning the Race: America's AI Action Plan, OMB Memorandum M-25-21, the DoW AIS Memo, the 2023 DoD DAAIS, and Air Force Doctrine Note (AFDN) 25-1, *Artificial Intelligence (AI)*. This instruction outlines the set roles, responsibilities, and processes that support the DoD AI Hierarchy of Needs; the primary goal of which is to accelerate the integration of AI technologies into military operations in an ethical, secure, and strategically aligned manner. AI governance provides an outline to implement mechanisms for evaluation, accountability, and transparency, encouraging the development and implementation of tailored guidelines for AI use. AI governance mitigates risks associated with AI deployment, such as a lack of objectivity, security vulnerabilities, loss of control of government data or models derived from government data, and ethical concerns, ensuring reliable AI systems that augment Airmen capabilities. Some of the competencies and purposes of AI governance are to:

2.1.1. Establish and implement comprehensive principles, policies, and frameworks to guide the responsible adoption and use of AI technologies and capabilities. For definitions and explanations of the AI technologies, concepts, and terminologies addressed by this ACCI, reference AFDN 25-1.

2.1.2. Ensure that AI systems are designed and maintained in full compliance with current laws and regulations. This includes integrating compliance measures into system development and operations, regularly reviewing and updating governance frameworks to address evolving legal standards, and incorporating best practices for transparency, accountability, and ethical usage throughout the AI lifecycle.

2.1.2.1. The approach to AI adoption in ACC is Human-Machine Teaming (HMT). HMT is the collaborative integration of human and AI capabilities to enhance operational effectiveness, employing constructs such as human-in-the-loop, human-on-the-loop, and human-out-of-the-loop to define levels of oversight.

2.1.2.2. Lifecycle management extends to the responsible decommissioning of legacy platforms. As necessary, HHQ will release guidance related to platform transitions to ensure security compliance, data preservation, and operational continuity.

2.1.2.3. The DoD AI Hierarchy of Needs (**Figure 2.1**) is a pyramid with quality data as its foundation, because all analytic and AI capabilities require trusted, high-quality data that meets rigorous standards of truthfulness and accuracy to deliver optimal mission-critical results and build offensive advantage. The next layer in the Hierarchy is insightful analytics, the foundational models and visualizations required for DoW leaders to understand their domains and the key variables impacting outcomes in those domains. At the top of the pyramid is Responsible AI (RAI), the Department's dynamic approach to the design, development, and use of AI capabilities that are consistent with the DoD AI Ethical Principles. For a detailed description of all layers of the pyramid, reference the 2023 DoD DAAIS.

2.1.2.4. Utilize the DoD AI Hierarchy of Needs as a strategic framework to assess ACC AI readiness. This approach not only identifies current capabilities and gaps in AI systems but also informs parallel initiatives for adopting comprehensive data and AI governance. By aligning assessments with the DoD AI hierarchical model, ACC can prioritize foundational infrastructure, establish robust oversight mechanisms, and ensure that governance policies evolve in tandem with technological advancements and operational requirements

**Figure 2.1. The DoD AI Hierarchy of Needs.**


2.1.3. Build and maintain a skilled and technically diverse workforce capable of understanding and explaining the AI models they are deploying. Governance frameworks will prioritize HMT to ensure AI systems augment, rather than replace, human decision-making, and function as an amplifier to Airmen capabilities.

2.1.4. Cultivate AI stewardship practices across various levels within ACC. Clearly define the roles and responsibilities of AI stewards, ensuring they are accountable for the effective management, governance, and ethical use of AI systems within their purview. These roles are detailed in **paragraph 4.6** and **Attachment 2**.

2.1.5. Encourage responsible AI acquisition, innovation, and adoption, IAW OMB Memorandum M-25-22, the U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, and the Defense Innovation Unit (DIU) *RAI Guidelines in Practice*.

2.1.6. Provide foundational oversight and technical baselines to:

2.1.6.1. Identify, assess, and mitigate risks associated with AI systems through comprehensive risk analyses that pinpoint potential threats, vulnerabilities, and unintended outcomes, ensuring adherence to rigorous safety, security, and ethical standards throughout their lifecycle. Develop and implement robust mitigation strategies to address these risks, while systematically evaluating AI applications and outputs to maintain compliance and performance.

2.1.6.2. Conduct thorough assessments to identify high-risk and high-impact AI applications, cataloging them in a detailed inventory that includes risk factors, usage contexts, and compliance requirements. Implement continuous monitoring procedures to track performance, detect emerging risks, and ensure adherence to safety, ethical, and regulatory standards, enabling proactive management of potential issues. For guidance on identifying high-impact AI and its specific requirements, refer to OMB Memorandum M-25-21.

2.1.6.3. Evaluate AI outputs by examining prediction accuracy, potential objectivity concerns, and input quality, cataloging outputs that require human review due to low accuracy, high risk, or poor data quality.

2.1.6.4. Align with the following DoD AI Ethical Principles for the design, development, deployment, and use of AI. The DOD's AI ethical principles build on the U.S. military's existing ethics framework based on the U.S. Constitution, Title 10 United States Code, *Armed Forces,* Law of War, existing international treaties and longstanding norms and values.

2.1.6.4.1. **Responsible:** All ACC personnel will exercise appropriate levels of judgment and care regarding the deployment and use of AI capabilities. Relevant ACC personnel shall oversee the development, deployment, and use of these systems, ensuring adherence to best practices, regulatory requirements, and ethical standards. This includes conducting thorough risk assessments, following established protocols, and continuously monitoring performance to guarantee that AI applications remain secure, reliable, and aligned with organizational values.

2.1.6.4.2. **Equitable:** ACC will take deliberate steps to ensure appropriate safeguards are in place to mitigate any unlawful discrimination, while prioritizing ideological neutrality in AI capabilities. This includes, but is not limited to, adopting best practices in data collection, model training, and evaluation.

2.1.6.4.3. **Traceable:** ACC's AI capabilities will be developed and deployed such that relevant ACC personnel possess an appropriate understanding of the underlying technology, development processes, and operational methods applicable to AI capabilities, including transparent and auditable methodologies, data sources, and design procedure and documentation.

2.1.6.4.4. **Reliable:** ACC's AI applications will be designed for specific, well-defined purposes. Their safety, security, and effectiveness will be rigorously validated through a comprehensive testing and assurance process integrated throughout the entire lifecycle—from initial development and deployment to ongoing maintenance. This process ensures that every AI application not only meets performance standards and

regulatory requirements but also remains reliable and secure in its defined operational context.

2.1.6.4.5. **Governable:** ACC will direct the design and engineering of AI systems to ensure they function as intended, and the frameworks and platforms include built-in governance safeguards. Relevant ACC personnel will continuously monitor these systems to detect and prevent unintended outcomes, and they are expected to use their discretion to disengage or deactivate any systems exhibiting unexpected behavior.

2.1.6.5. Implement privacy-enhancing technologies and security measures to protect sensitive data and ensure the secure deployment of AI systems.

**2.2. Background.** AI technologies are rapidly advancing, holding immense potential to enhance capabilities within the DoW, DAF, and ACC. However, it also presents significant risks of misuse that could jeopardize national security. Responsible governance and stewardship are crucial in harnessing the potential of AI and strengthening strategic advantage, while effectively mitigating risks associated with the adoption of these technologies

**2.3. Purpose.** This instruction will further direct and guide ACC in the adoption of AI governance practices, while aligning them with key mission and ethical objectives. This instruction will:

2.3.1. Address AI governance challenges for all ACC personnel, processes, structures, and technologies.

2.3.2. Ensure the technical framework for implementation of AI governance is aligned with DoW and DAF standards.

2.3.3. Identify key roles and responsibilities and define annual reporting. Collect metrics to track AI governance implementation actions, adherence to standards and policies, and the collective enterprise effects.

**2.4. Strategy and Framework.** Implementing AI governance is a collective effort that requires senior leadership advocacy, proactive leadership, and engagement at all levels. The following foundational principles will be implemented across the entire AI lifecycle.

2.4.1. **RAI Governance:** Ensure a disciplined governance structure with defined processes for oversight and accountability. Clearly articulate ACC guidelines on RAI and associated incentives.

2.4.2. **Warfighter Trust:** Build warfighter trust by embedding AI into training and operational environments. Establish a testing, evaluation, verification, and validation framework that integrates real-time monitoring, algorithm confidence metrics, and user feedback to ensure trusted and reliable AI capabilities. Implement explainable AI to ensure warfighters can understand, appropriately trust, and effectively manage AI systems. This includes developing transparent AI models that provide interpretable outputs and decision-making processes, enabling warfighters to comprehend system behavior and align it with mission objectives. Integrate HMT into education and training programs to enhance user confidence and operational effectiveness.

2.4.3. **Requirements Validation:** Integrate RAI principles into all applicable AI requirements to ensure their incorporation into ACC's AI capabilities.

2.4.4. **Responsible AI Ecosystem:** Build an AI ecosystem to improve collaboration between and promote the ability of ACC entities to develop and deploy AI systems in a way that prioritizes these RAI foundations.

2.4.4.1. Standardize on enterprise-level AI platforms to ensure consistent governance, security, and interoperability. As part of this strategy, ACC will transition from legacy capabilities to enduring enterprise services to leverage shared, secure infrastructure and reduce duplication of effort, emphasizing a "connect once, enable many" approach.

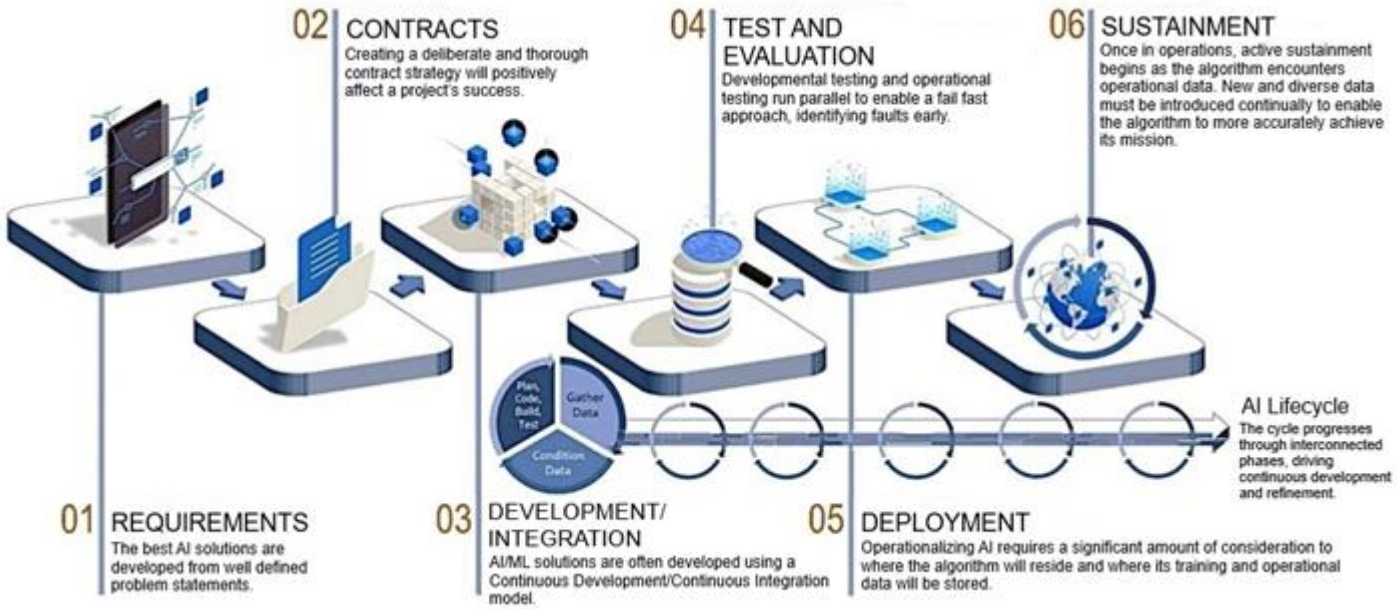
2.4.4.2. Reduce risk by centralizing internal AI model development for continuous experimentation, while establishing rapid feedback loops to implement output–based adjustments to the models. Rigorously tested and approved capabilities will receive clear pathways to sustainment and wide-scale adoption.

2.4.4.3. When proceeding through the AI product lifecycle, utilize the DIU *RAI Guidelines in Practice* to provide a clear, efficient inquiry process and comprehensive guidance on key considerations, consistent with higher level Executive policies and direction.

2.4.4.4. ACC ISR Enterprise will follow this ACCI when not in conflict with laws specific to intelligence, or the policy, guidance and standards issued by the Office of the Director of National Intelligence (ODNI) or the Headquarters of the Air Force A2.

2.4.5. **AI Product and Acquisition Lifecycle:** Synchronize enterprise RAI implementation for the AI product throughout the acquisition lifecycle by means of a systems engineering and risk management approach IAW OMB Memorandum M-25-22 and the DAF Chief Data and AI Office (CDAO) *AI Acquisitions Guidebook,* and the acquisition acceleration mandates of the DoW AIS Memo. AI acquisitions must include clauses that require vendors to comply with DoW and DAF policy, as well as restricting vendors from training or fine-tuning foundation models on government-furnished data without explicit, prior government approval.

**Figure 2.2. AI Product Lifecycle.**



## Chapter 3

## DATA & AI GOVERNANCE BODY

**3.1. Managing Risk.** To maintain velocity and outpace our adversaries, ACC will adopt an agile governance model. All stakeholders will have the ability to identify and present risks, while limiting the barriers inherent to overly bureaucratic governance models. Governance bodies will be implemented to ensure the consistency of data and AI governance across ACC.

**3.2. Disciplines.** These bodies function to inform decisions, shape a more data-driven culture, enable effective adoption and management of AI within ACC, and facilitate a collaborative ACC data and AI environment through consistent communication.

**3.3. Framework.** ACC's data and AI governance will be designed with the following bodies to ensure a successful framework is established.

3.3.1. **ACC Data & AI Board:** The ACC Data & AI Board, hereafter known as the Board, is the primary and highest authority for ACC data and AI governance. The Board is responsible for the oversight and support of all ACC data and AI governance activities. The Board will:

3.3.1.1. Consist of director-level representatives (primary members), data and AI stewards (advisors), stakeholders, and subject matter experts across ACC.

3.3.1.2. Align board member roles and responsibilities with the charter endorsed by the Commander of Air Combat Command (COMACC), which establishes Board scope, activities, and goals. Charter must be reviewed/updated annually or more frequently when deemed necessary.

3.3.1.3. Review ACC personnel and NAF/Wing (T-3) waivers and Plans of Actions and Milestones (POAM) and provide enterprise decisions. This applies to any situation in which a commander or wing requires clarification or a second opinion regarding waiver applicability.

3.3.1.4. When applicable, request and secure funding for data and AI governance and data and AI governance sponsored activities recommended by but not limited to: HHQ Data Governance Councils, DoW CDAO, and/or the DAF CDAO.

3.3.1.5. Upon the release of HHQ guidance or policy, guide units in order to facilitate adherence to the directives and implement necessary actions to ensure compliance. ACC ISR units must refer to the Intelligence Data Governance Council for such.

3.3.1.6. When applicable, advise on and approve NAF rules and procedures for implementation of data and AI governance.

3.3.1.7. Establish instructions and guidelines for all units regarding documentation and compliance requirements mandated by this instruction.

3.3.1.8. Manage data and AI governance initiatives (e.g., development of guidance or metrics), issues, and escalations. Provide guidance and support in planning the adoption of metadata standards.

3.3.1.9. Serve as the final authority on disputes, such as disagreements between ACC organizations over business glossary definitions and formatting.

3.3.1.10. Create and direct temporary working groups with specialized expertise in targeted areas of data and AI governance, each with well-defined goals and objectives aligned with the Board's intent. The Board will appoint a lead member to oversee scheduling, planning, and facilitating meetings, as well as coordinating research and reporting outcomes to the Board. These groups will provide focused guidance and advice on specific aspects of data and AI governance, ensuring effective support for the Board's oversight and decision-making processes.

3.3.2. **ACC Command Data & AI Office (ACC/CDAO):** The ACC/CDAO will focus on enterprise-level mission outcomes through instituting and operationalizing data and AI definitions and management standards across mission areas. These efforts will reduce integration and interoperability costs, ensure data interoperability across mission and functional boundaries, and promote machine understandable data for AI usage at scale across the enterprise. The ACC/CDAO will:

3.3.2.1. Coordinate and define stewardship and additional roles within the ACC Data & AI Governance Program.

3.3.2.2. Provide applicable support to the governing bodies, assigned roles, working groups, and/or any organization under the ACC Data & AI Governance Program.

3.3.2.3. Maintain and publish all source documents related to data and AI governance (e.g., data and AI steward appointment letters, standards, definitions, glossaries, policies, directives, models, domain ontologies, etc.).

## Chapter 4

## ROLES AND RESPONSIBILITIES

**4.1. Purpose.** This instruction will outline the roles relevant to ACC data and AI governance, as well as outline the scope of the responsibilities and competencies applicable to each role.

**4.2. DAF CDAO.** Develop and implement strategies and DAF-level policies for enterprise data management, data and AI capability and platform transitions, mandated AI Risk Management Frameworks, and responsible/ethical AI.

**4.3. ACC/CDAO.** ACC/CDAO will establish and manage the ACC Data & AI Governance Program IAW guidance from DoW and DAF CDAO, and will execute its duties with the urgency and empowerment directed by the DoW AIS Memo. Additionally, the ACC/CDAO will:

4.3.1. Ensure ACC data and AI systems meet DoW and DAF policies, standards, guidance, and directives.

4.3.2. Represent ACC in higher-level forums or working groups as needed or directed.

4.3.3. Advise on tools and software capabilities to support data and AI governance and management. This includes promoting the adoption of DAF-approved enterprise services such as GenAI.mil - the designated platform for generative AI capabilities - as well as guiding units through the decommissioning of legacy or pathfinder systems.

4.3.4. Establish a unified platform to operationalize data and AI governance. Integrating standardized data schemas, metadata repositories, and AI model registries will ensure interoperability, traceability, and compliance with DoW and DAF standards, and mechanisms for reporting and addressing misuse of AI through auditable logs and incident tracking procedures.

4.3.5. Advise on and drive the upskilling of the force through training, literacy, human resources, and organizational changes to support data and AI governance and management and cultivate an AI-first culture. Links for relevant training will be maintained on the ACC/CDAO SharePoint page: usaf.dps.mil/teams/CDAO/Upskilling.aspx

4.3.6. Coordinate with relevant stakeholders to establish minimum data and AI stewardship training requirements.

4.3.7. Advise and support ACC in the management and execution of data and AI governance and management initiatives.

4.3.8. Coordinate with relevant stakeholders to operationalize detailed guidelines for metadata tagging IAW the *DoD Metadata Guidance*, including a standardized set of metadata fields and instructions on how to apply them consistently across all ACC data assets. For additional information related to metadata standards, reference **Attachment 3**.

4.3.9. Develop and maintain a comprehensive command data dictionary that standardizes definitions, formats, and usage guidelines for all ACC data assets, ensuring consistency, interoperability, and compliance with DoW and DAF data governance standards

4.3.10. Clearly define the roles and responsibilities of data and AI stewards, ensuring they are accountable for proper governance, cataloging, and tagging of data assets and the ethical, responsible, and effective deployment of AI capabilities.

4.3.11. **Roles within the ACC/CDAO:**

4.3.11.1. **The Command Data Officer** is the single point of contact to the DAF CDAO for all data management-related activities within their organizational purview. The Command Data Officer will:

4.3.11.1.1. Advise the COMACC and other Senior Leaders on policies and guidance related to data management.

4.3.11.1.2. Champion and implement enterprise data management and sharing objectives.

4.3.11.1.3. Communicate data initiatives and activities within ACC.

4.3.11.1.4. Inform DAF CDAO of data-related matters across the enterprise to eliminate duplicative efforts and enable enterprise-wide capabilities.

4.3.11.1.5. Ensure data registration and tagging IAW DoW data implementation guidance.

4.3.11.1.6. Recommend prioritization of data requirements, proposed risk mitigation, and acceptance criteria.

4.3.11.1.7. Regularly collaborate with enterprise data officers to align on objectives and best practices. Additionally, engage with ACC personnel to identify data management requirements and operational processes, informing high-level guidance.

4.3.11.2. **The Command AI Officer** is the single point of contact to the DAF CDAO for all AI governance-related activities within their organizational purview. The Command AI Officer will:

4.3.11.2.1. Champion and implement enterprise AI management and sharing objectives.

4.3.11.2.2. Advise the COMACC and other Senior Leaders on policies and guidance related to AI.

4.3.11.2.3. Ensure ACC AI projects and programs are developed and compliant in accordance with higher-level mandated requirements and AI ethical principles adopted across DoW and the DAF.

4.3.11.2.4. Maintain comprehensive oversight of AI systems post-deployment, including ongoing performance evaluation and risk mitigation activities.

4.3.11.2.5. Review and advise the merit, sufficiency, and completeness of enterprise-wide AI solutions that require investment.

4.3.11.2.6. Identify or develop AI-related competencies, knowledge, and skills for roles within ACC.

4.3.11.2.7. Prioritize AI interoperability with external mission partners and stakeholders, when appropriate and in compliance with existing policy and guidance.

4.3.11.2.8. Develop and provide ACC guidance and governance related to AI not otherwise directed by higher authority but required at the MAJCOM level.

4.3.11.2.9. Inform DAF CDAO of AI-related matters across the enterprise to eliminate duplicative efforts and enable enterprise-wide capabilities.

4.3.11.2.10. Inform ACC units of AI-related matters across the MAJCOM to eliminate duplicative efforts and enable ACC-wide capabilities.

4.3.11.2.11. Ensure AI use case and model registration is done IAW DoW guidance and within DAF CDAO platforms.

4.3.11.2.12. Recommend prioritization of AI requirements, proposed risk mitigation, and acceptance criteria.

4.3.11.2.13. Regularly collaborate with enterprise AI officers to align objectives and best practices. Additionally, engage with ACC personnel to identify AI system requirements and operational processes, informing high-level guidance.

4.3.11.2.14. Coordinate AI waivers between ACC units and DAF CDAO.

**4.4. ACC NAF, Wing, Group, and Squadron Commanders.** Commanders will be responsible for ensuring their respective units are implementing all required data and AI governance mandates, including compliance with the requirements outlined in this instruction in **paragraph 4.5**, "ACC NAF/ Wing/Group/Squadron Commander's Compliance Requirements" below. ACC NAF, Wing, Group and Squadron Commanders who have not fully implemented higher DoW and/or DAF policy or guidance for data and AI governance will adhere to Board published directions regarding compliance, reporting, timelines, and POAM/Waiver processes and requirements. Detachment Commanders will adhere to these requirements if the Detachment is operationally controlled by ACC.

4.4.1. Dependent upon operational need, Commanders will establish data and AI stewardship teams and working groups, in writing, to ensure compliance with ACC's data and AI governance. **(T-3)** Reference **Attachment 2.**

4.4.2. May publish local data and AI governance policies aligned and in compliance with higher-level authorities.

4.4.3. Implement and enforce procedures to report statistical bias or misuse of AI to the appropriate oversight offices, along with supporting procedures for response to such reports.

4.4.4. Must use annual programming activities, site visits, and other means to highlight data and AI governance resource shortfalls through their chain of command to the Board. **(T-3)**

**4.5. ACC Staff and NAF/ Wing/Group/Squadron Commander's Compliance Requirements.** Templates for required documents listed below are located on the ACC/CDAO SharePoint page: **https://usaf.dps.mil/teams/CDAO/SitePages/ProductsAndResources.aspx** (If you have difficulty accessing this URL, please email the ACC/CDAO office at: **acc.a6d.cdao@us.af.mil** ). The Board will provide the current URL to acquire templates for required documents listed below should SharePoint not be active/available.

4.5.1. Must comply with DoW, DAF, and ACC related instructions, policies, directives, publications, and governance bodies. **(T-0)**

4.5.2. Ensure data and AI governance requirements are included in acquisition efforts.

4.5.3. Ensure minimum DoW metadata standards are met to align data with VAULTIS principles. **(T-2)** Reference **Attachment 3.**

4.5.4. Produce/maintain data flow architecture schema/mapping of all data sets. **(T-3)**

4.5.5. Ensure participation in the appropriate data and AI governance forums or working groups as directed by ACC data and AI governance bodies. **(T-2)**

4.5.6. IAW the DepSecDef Memorandum, *Creating Data Advantage*, catalog all data at the lowest echelon while ensuring data is discoverable and shared beyond the unit. Cataloging is necessary to ensure compliance with this instruction and to provide an accurate and up-to-date data inventory.

4.5.7. IAW SAF/CN Memo, *Establishing Policy to Enable Compliance with Federal Artificial Intelligence Registration Guidance*, enforce registration and processing compliance of all AI use cases and models using the official DAF AI repositories for each.

4.5.8. Assign priority designations to datasets, considering the following data factors: criticality, sensitivity, quality, lineage, and HHQ and/or ACC requirements. Once high priority datasets have been identified, governance policies and procedures can be established to ensure that data is managed effectively and efficiently.

4.5.9. Complete and submit data and AI maturity self-assessment results, as detailed in **paragraph 4.7**.

4.5.10. Ensure training requirements are met and tracked within their organization.

4.5.11. Manage organizational transitions from legacy systems to approved enterprise services.

**4.6. Data and AI Stewardship.** Stewardship is the proactive accountability and responsibility for processes that ensure effective control and use of data assets and management of AI systems. Responsibilities will differ between the strategic, operational, and tactical levels, as well as disciplines and mission functions. At the strategic level, stewards oversee broad domains, while at lower levels, they focus on specific functions or tasks. Stewardship roles may be integrated into existing, similar positions or designated as a full-time role based on mission and resources. The best stewards are found, not made, and Commanders will appoint appropriate stewards to manage data assets in support of mission requirements. Each of the following roles and responsibilities are considered “best practices” and, as such, are essential to performing data and AI stewardship in a manner that facilitates the transformation of the DoW into a data-centric and AI-enabled enterprise. Reference **Attachment 2.**

4.6.1. **Stewardship Teams** are led by the senior-level data and AI stewards across ACC. They consist of experts across a range of disciplines – operations, IT, data security, knowledge management, AI fundamentals, etc., but can be appointed from any Air Force Specialty Code /Civilian job coded series at the Commander’s discretion. Teams focus on implementing data and AI governance within their organization’s scope and responsibilities.

4.6.2. **Data Stewardship Responsibilities:**

4.6.2.1. Complete the requisite training to fill the role. Reference **paragraph 4.3.5** for training links.

4.6.2.2. Manage data sets that the unit/organization has accountability and authority over. Provide reporting updates to the Board when data lines are specifically addressed by Board efforts.

4.6.2.3. Provide subject matter expertise in the context of mission execution and criteria for adhering to data governance and policies to guide effective data use.

4.6.2.4. Ensure data under their area of responsibility is properly governed, cataloged, and meets quality and accessibility standards to enable consistent and reproducible analytical outcomes.

4.6.2.5. Provide data governance and implementation feedback and recommendations through their chain of command and/or NAF/Wing level data and AI governance bodies.

4.6.2.6. Facilitate the integration of data management systems and workflows with analytics and AI capabilities.

4.6.2.7. **NAF and Wing Data Stewards Will:**

4.6.2.7.1. Represent their NAF or Wing data governance working groups within governance forums or working groups directed by ACC data governance bodies (designated OPR).

4.6.2.7.2. Develop processes to ensure data tagging occurs in compliance with data standards mandated by the Board.

4.6.2.8. **Group and Squadron Data Stewards Will:**

4.6.2.8.1. Adhere to higher-level policies and processes to ensure data tagging in compliance with DoW, DAF, and NAF/Wing requirements.

4.6.2.8.2. Stewards at this level are to delegate data tagging responsibilities to data custodians that hold purview over their specific mission area.

4.6.3. **AI Stewardship Responsibilities:**

4.6.3.1. Complete the requisite training to fill the role, as well as continue ongoing education in AI advancements related to their role. Reference **paragraph 4.3.5** for training links.

4.6.3.2. Provide subject matter expertise in the context of mission execution and criteria for adhering to AI governance policies.

4.6.3.3. Prioritize ethical considerations by ensuring AI systems are transparent, fair, and objective, with a methodology for ongoing assessment of AI outputs and their impact on data privacy and security.

4.6.3.4. Identify AI model owner and sustainment plan.

4.6.3.5. Ensure AI models are added to the DAF repository of record for tracking use case requirements and verify that DoW mandated information is included. AI models supporting intelligence or used in intelligence production will be added to the appropriate ODNI repository due to OPSEC and potential classification concerns.

4.6.3.6. Develop and analyze use cases that are best addressed by AI solutions promoted via requirement process and/or the Board.

4.6.3.7. **NAF and Wing AI Stewards Will:**

4.6.3.7.1. Represent their NAF or Wing AI governance working groups within governance forums or working groups directed by ACC AI governance Bodies (designated OPR).

4.6.3.7.2. Develop processes to ensure the quality, integrity, and ethical use of data used in AI systems occurs in compliance with data standards mandated by the Board.

4.6.3.8. **Group and Squadron AI Stewards Will:**

4.6.3.8.1. Adhere to higher-level policies and processes to ensure responsible use of AI in compliance with DoW, DAF, and NAF/Wing requirements.

4.6.3.8.2. Collaborate with data custodians to ensure data tagging adheres to standards that optimize AI model training, performance, and interoperability.

4.6.4. **Shared Endeavor.** Data stewardship and AI stewardship are distinct yet interconnected tasks, each with specific responsibilities and focus areas. They become integrated at various levels, and this integration is essential to ensure AI models are effectively harmonized with data and analytics outputs, fostering a collaborative approach that aligns data stewardship practices with analytics and AI capabilities. This shared endeavor promotes the responsible use of data, the reliability of analytical insights, and the ethical application of AI systems. Depending on the mission, designated personnel will serve as data stewards, focusing on data management; others as AI stewards, overseeing model design, deployment, and use; and some as both, integrating data and AI oversight. Some efforts that may overlap data and AI stewardship roles include:

4.6.4.1. Support their Commander’s data and AI governance policies and implementation actions and represent the Commander’s equities in internal and external forums.

4.6.4.2. Adhere to guidance, policy, and directives published by the Board, as well as serve as liaisons between their organization and the Board.

4.6.4.3. Facilitate systems that enable interoperability, allowing for seamless exchange between data repositories, analytics platforms, and AI systems.

4.6.4.4. Integrate AI capabilities into data management processes for enhanced data quality management, pattern recognition, and predictive analytics.

4.6.4.5. Conduct feasibility analysis on AI use case requirements for data availability, access, sufficiency, and quality, and validate analytic algorithms to ensure the reliability and reproducibility of insights powering AI systems.

4.6.4.6. Participate in working groups established by the Board to collaborate on compiling lessons learned from data and AI stewardship efforts, fostering data and AI interoperability, and refining stewardship practices to optimize the performance and interoperability of analytics and AI systems.

**4.7. Maturity Assessments.** A comprehensive annual assessment of the respective ACC organization's data and AI maturity will be conducted by ACC Staff and NAF/ Wing/Group/Squadron Commanders for the purpose of identifying strengths, weaknesses, and opportunities for improvement to ensure alignment with strategic goals and industry best practices. The assessment will cover all data and AI-related activities, including data governance, data

quality, data integration, AI model development, deployment, monitoring, and ethical compliance. ACC CDAO will relay HHQ guidance on assessment specifications as they are released.

4.7.1. **Data Assessments:**

4.7.1.1. **Data Governance:** Evaluate data governance framework, policies, and procedures to ensure effective data stewardship and compliance with privacy and security regulations.

4.7.1.2. **Data Quality:** Analyze the quality and accuracy of data assets, assess data validation and verification processes, and identify areas for improvement in data quality and integrity.

4.7.1.3. **Data Integration:** Evaluate data integration capabilities, including tools, technologies, and methodologies, review data integration workflows and data flow diagrams, and identify opportunities for streamlining and improving data integration processes.

4.7.2. **AI Assessments:**

4.7.2.1. **AI Model Development:** Assess AI model development practices and methodologies, evaluate the availability and quality of training data, review feature engineering and model selection approaches, and identify opportunities to enhance AI model development processes.

4.7.2.2. **AI Model Deployment:** Evaluate practices for deploying AI models into production, assess the scalability and performance of deployed models, ensure separation of AI outputs from data collections, review model versioning and monitoring approaches, and identify areas for improvement in AI model deployment processes.

4.7.2.3. **AI Model Audits and Testing:** Analyze practices for monitoring the performance of deployed AI models, assess the effectiveness of model performance metrics and thresholds to validate reliability, utilizing methods such as edge case testing, review approaches to detecting and addressing model drift, and identify opportunities to enhance AI model monitoring capabilities.

4.7.2.4. **Ethical Considerations:** Evaluate ethical guidelines and policies for AI usage, assess the truthfulness, transparency, and interpretability of AI models, review approaches to ensuring objectivity and algorithmic accountability, and identify blind spots in ethical compliance related to AI. Assess minimum-risk management practices for those categories of AI that are identified as high-risk or high-impact, including pre-deployment risk assessments.

4.7.3. The assessment from the ACC/CDAO is not to replace any existing assessments from respective units' higher authorities (e.g., aircraft maintenance Integrated Maintenance Data System standards, etc.). If a unit is already abiding by their higher authority's data standards, the ACC/CDAO only requires that all ACC datasets be registered in their authorized central data registry set forth by ACC/CDAO or DAF CDAO; moreover, they must abide by the minimum metadata standards set forth by DoW. Due to the unique nature of operational intelligence data, ISR datasets meant for their unique catalog are exempt.

ADRIAN L. SPAIN
General, USAF
Commander

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

10 USC, Armed Forces

ACCMAN 14-422, *Intelligence Data Governance,* 24 October 2023

AFDN 25-1, *Artificial Intelligence (AI)*, 8 April 2025

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

*DAF Application Program Interface (API) Reference Architecture*, October 2024

DAF CDAO, *AI Acquisitions Guidebook,* March 2024

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

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

DepSecDef Memorandum, *Creating Data Advantage,* 5 May 2021

DIU, *Responsible AI Guidelines in Practice*, March 2020

DoD Data Strategy, 2020

DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, 27 June 2023

DoW Memorandum, *Artificial Intelligence Strategy for the Department of War, 9 January 2026*

NIST AI 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, 26 January 2023

NIST AI 100-3, *The Language of Trustworthy AI: An In-Depth Glossary of Terms*, March 2023

OMB Memorandum M-25-21, *Accelerating Federal use of AI through Innovation, Governance, and Public Trust*, 3 April 2025

OMB Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government*, 3 April 20205

SAF/CN Memorandum, *Establishing Policy to Enable Compliance with Federal Artificial Intelligence Registration Guidance*, 6 November 2024

U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*,* June 2022

***Prescribed Forms***

None

***Adopted Forms***

DAF Form 847, *Recommendation for Change of Product*

***Abbreviations and Acronyms***

**ACC**—Air Combat Command

**ACCI**—Air Combat Command Instruction

**ACCMAN**—Air Combat Command Manual

**AFDN**—Air Force Doctrine Note

**AI/ML**—Artificial Intelligence and Machine Learning

**API**—Application Programming Interface

**CDAO**—Chief Data and Artificial Intelligence Office

**DAF**—Department of the Air Force

**DAFMAN**—Department of the Air Force Manual

**DIU**—Defense Innovation Unit

**DML**—Data Management Lexicon

**DMR**—Data Maturity Reports

**DoD**—Department of Defense

**DoW**—Department of War

**IAW**—In Accordance With

**ISR**—Intelligence, Surveillance, and Reconnaissance

**IT**—Information Technology

**HHQ**—Higher Headquarters

**HMT**—Human-Machine Teaming

**MAJCOM**—Major Command

**NAF**—Numbered Air Force

**NIST**—National Institute of Standards and Technology

**ODNI**—Office of the Director of National Intelligence

**OPR**—Office of Primary Responsibility

**OPSEC**—Operational Security

**POAM**—Plan of Action & Milestones

**RAI**—Responsible Artificial Intelligence

**USAF**—United States Air Force

**VAULTIS**—Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, Secure

***Office Symbols***

**ACC/CDAO**—Air Combat Command/Command Data & Artificial Intelligence Office

**DAF CDAO**—Department of the Air Force Chief Data and Artificial Intelligence Office

*Terms*

**Algorithm**—Precise rules for transforming specified inputs into specified outputs in a finite number of steps. (Source: NIST Glossary)

**Analytics**—The systematic computational analysis of data or statistics to discover and identify meaningful information and trends. (Source: IC DML)

**Anonymization**—Process that removes the association between the identifying dataset and the data subject in such a way that does not harm the usability of the data. (Source: NIST Glossary)

**Application Programming Interface**—A software contract between applications, expressed as a collection of methods or functions. It defines the available executable functions and serves as the intermediary interface between the applications. (Source: NIST Glossary)

**Artificial Intelligence**—The ability of machines to perform tasks that normally require human intelligence- for example- recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action- whether digitally or as the smart software behind autonomous systems. (Source: 2018 DoD AI Strategy)

**Artificial Intelligence Governance**—A system of laws, policies, frameworks, practices and processes that enables stakeholders to implement, manage, oversee and regulate the development, deployment, and use of AI technology. It also helps manage associated risks to ensure AI aligns with stakeholders' objectives, is developed and used responsibly and ethically, and complies with applicable legal and regulatory requirements. (Source: NIST Glossary)

**Artificial Intelligence Maturity Assessment**—A comprehensive evaluation of the quality and/or state of an organization's capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with relevant Federal law, regulation, and policy on AI. (Source: OMB Memo M-25-21)

**Artificial Intelligence System**—An engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. (Source: NIST Glossary)

**Bias**—An effect which deprives a statistical result of representativeness by systematically distorting it, as distinct from a random error which may distort on any one occasion but balances out on the average. (Source: NIST Glossary)

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

**Cataloging**—The process of curating (gathering, organizing, maintaining, presenting) a collection of metadata about resources. (Source: IC DML)

**Collection**—Any information or data, both in its final form, and in the form when initially gathered, acquired, held, or obtained that is potentially relevant to mission need. This includes information or data obtained directly from its source, regardless of whether the information or data has been reviewed or processed. (Source: IC DML)

**Command Data Officer**—Designated Senior Official within each agency responsible for the management of data as an asset and the establishment and enforcement of data-related strategies, policies, standards, processes, and governance. (Source: IC DML)

**Command AI Officer**—The single point of contact to the Department of the Air Force Chief Data and Artificial Intelligence Office for all AI governance-related activities within their organizational purview.

**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. (Source: IC DML)

**Data & AI Governance Council**—A decision making and/or policy making council of senior managers, chaired by the Command Data and AI Officer, who are responsible for the highest tier of data & AI governance in an agency. The Data & AI Governance Council oversees or manages data & AI governance initiatives (e.g., development of policies or metrics), issues and escalations. Monitors results to ensure the desired outcomes and business value from data and AI management activities. (Source: IC DML)

**Data as a Strategic Asset**—Data that may be relevant to one or more ACC elements for analytics purposes. ACC data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage. (Source: 2020 DoD Data Strategy)

**Data Asset**—Data maintained and secured as a shared, critical, inexhaustible, durable, and strategic resource with the expectation of future value and benefits. Examples of data assets include databases, documents, data returned as web content, application/system output files and records. (Source: IC DML)

**Data Governance**—A set of processes, including policies, people, practices, and technologies, that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority, management and decision-making parameters related to the data produced or managed by the enterprise. (Source: NIST Glossary)

**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. (Source: IC DML)

**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. (Source: IC DML)

**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 tradecraft professionals following established disciplines and functions. (Source: IC DML)

**Data Maturity Assessment**—A comprehensive evaluation of the quality and/or state of development of either data or the data management activities, processes, and tools being used to perform data management functions. (Source: DoD Data Stewardship Guidebook)

**Data Quality**—The degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use. (Source: IC DML)

**Dataset**—One or more data objects that share common properties and characteristics and are managed as a unit. (Source: IC DML)

**Data Silo**—Isolated repositories of data that are not easily accessible or shared with other systems or departments within an organization.

**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. (Source: IC DML)

**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). (Source: IC DML)

**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. (Source: IC DML)

**DoD AI Hierarchy of Needs**—A pyramid with quality data as its foundation, the next layer in the Hierarchy is insightful analytics and metrics, and the top of the pyramid is Responsible AI. (Source: 2023 DoD Data, Analytics, and AI Adoption Strategy)

**Edge Cases**—Situations in which the AI will fail or be insufficient to deal with the external realities of a situation. Ideally, testing should deliberately seek to identify and expose those edge cases to either improve the AI model or limit what the AI is asked to do. More complex situations potentially present an infinite number of edge cases, which makes reliability testing increasingly difficult, and failure in the field more likely. (Source: AFDN 25-1*)*

**Explainability**—A characteristic of an AI system in which there is provision of accompanying evidence or reasons for system output in a manner that is meaningful or understandable to individual users (as well as to developers and auditors) and reflects the system's process for generating the output; The extent to which AI decisioning processes and outcomes are reasonably understood. (Source: NIST Glossary)

**High—Impact AI**—AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on: an individual or entity's civil rights, civil liberties, or privacy; an individual or entity's access to education, housing, insurance, credit, employment, and other programs; an individual or entity's access to critical government resources or services; human health and safety; critical infrastructure or public safety; or strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government. (Source: OMB Memo M-25-21)

**Human—Machine Teaming**—The collaborative integration of human and AI capabilities to enhance operational effectiveness, where Airmen leverage AI's rapid data processing and analytical strengths alongside human intuition, reasoning, and contextual judgment. (Source: AFDN 25-1*)*

**Human—in-the-Loop**—The machine makes recommendations, and the person makes the decision. (Source: AFDN 25-1*)*

**Human—on-the-Loop**—The machine makes recommendations, and the machine recommendation will be implemented unless the person vetoes the machine action. (Source: AFDN 25-1*)*

**Human—out-of-the-Loop**—The machine makes the decision, and the person cannot override the machine's action. (Source: AFDN 25-1*)*

**Intelligence Data**—Refers to information collected, analyzed, and disseminated by intelligence agencies to support national security and decision-making processes. It encompasses a wide range of information obtained through multi-INT sources. Intelligence data is typically processed, analyzed, and transformed into actionable intelligence to inform strategic, operational, and tactical decisions.

**Interoperability**—The ability of software or hardware systems or components to operate together successfully with minimal effort by end user. (Source: NIST Glossary)

**Interpretability**—The ability to understand the value and accuracy of system output. Interpretability refers to the extent to which a cause and effect can be observed within a system or to which what is going to happen given a change in input or algorithmic parameters can be predicted. (Source: NIST Glossary)

**Lineage**—A description of data's pathway from its source to its current location and the alterations made to the data along that pathway, which should be represented as a reproducible ancestry of the data object. Lineage can include traceability between parent and children data objects. (Source: IC DML)

**Machine Learning**—A branch of AI that focuses on the development of systems capable of learning from data to perform a task without being explicitly programmed to perform that task. Learning refers to the process of optimizing model parameters through computational techniques such that the model's behavior is optimized for the training task. (Source: NIST Glossary)

**Metadata**—Literally, "data about data"; Data employed to annotate other data with descriptive information, possibly including their data descriptions, data about data ownership, access paths, access rights, and data volatility. (Source: NIST Glossary)

**Mission Data**—Data gathered, acquired, generated, held, or obtained during mission activities by an organization (e.g., IC element, DoW element, law enforcement element) to satisfy mission (e.g., intelligence, defense, law enforcement) needs and which can be shared across systems and organizations working toward the same mission. This data includes, but is not limited to, observations, recordings, images, signals, measurements, and signatures of physical or digital attributes and events. (Source: IC DML)

**Model**—A core component of an AI system used to make inferences from inputs to produce outputs. A model characterizes an input-to-output transformation intended to perform a core computational task of the AI system (e.g., classifying an image, predicting the next word for a sequence, or selecting a robot's next action given its state and goals). (Source: NIST Glossary)

**Objectivity**—Based on facts and not influenced by personal beliefs or feelings; freedom from bias.

**Ontology**—A formal representation of a domain of knowledge. It is comprised of a taxonomy as an integral part, with an underlying vocabulary including definitions of terms representing

universals, defined classes, and axioms from which rational arguments can be made. (Source: IC DML)

**Privacy—Enhancing Technology**—A coherent system of Information and Communications Technology measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. (Source: NIST Glossary)

**Responsible AI**—AI that operates IAW the DoD AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, Governable. (Source: Memo, Implementing Responsible AI in the DoD)

**Risk**—The composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event. The impacts, or consequences, of AI systems can be positive, negative, or both and can result in opportunities or threats. (Source: NIST Glossary)

**Stakeholder**—Any individual, group, or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. (Source: NIST Glossary)

**Terminology—Note:** To promote consistency within the national security community, the DoW and DAF utilize the data management terminology codified in the ODNI Data Management Lexicon (IC DML) and AI terminology with NIST AI 100-3, *The Language of Trustworthy AI: An In-Depth Glossary of Terms.*

## Attachment 2

## POTENTIAL DATA AND AI STEWARDSHIP ROLES

### A2.1. Types of Stewards:

A2.1.1. **Chief Data Stewards** lead Data Governance Offices and chair Data Governance Councils. Participate in higher-level data governance bodies to ensure compliance with upper-level policies, standards, guidance, and directives.

A2.1.2. **Executive Data Stewards** are senior leaders with voting power who serve on Data Governance Councils and include an IT Lead.

A2.1.3. **Domain Data Stewards** have oversight of a specific data domain within an enterprise (e.g., INT-Specific, Combatant Commands, Platforms, etc...).

A2.1.4. **Coordinating Data Stewards** lead and represent Data Steward Teams under their organizational structure. Normally reside at the wing & group levels.

A2.1.5. **Data Managers** are members who assume approval authority for decisions about data within their scope of responsibility; maintain the quality of the data within their domain.

A2.1.6. **Data Custodians** perform mission data-related tasks such as collecting, tagging, and processing data, and grant individual users access to additional information beyond that of general systems, applications, and the permissions to perform actual functions where appropriate.

A2.1.7. **Data Stewards** , at the organization level, are recognized subject matter experts accountable for a subset of data. Data stewards will ensure data sets under their responsibility are appropriately tagged, curated, and cataloged. They coordinate with stakeholders to define and control data; moreover, maintain data names, definitions, data integrity rules, and domain values; ensure compliance with legal and policy requirements, and conformance to data policies and standards; ensure application of appropriate security controls; and analyze and improve data quality. Data Stewards appoint and provide guidance to Data Managers in their Sub Portfolio or organization.

A2.1.7.1. **Technical Data Stewards** are often IT professionals that provide technical expertise around source systems, Extract, Transform, and Load processes, data stores, data warehouses, and business intelligence tools. Technical Data Stewards produce/maintain data flow schema & mapping of data within their organization.

A2.1.7.2. **Collection Stewards** are responsible for collected data to ensure dissemination, discoverability, accessibility, and interoperability by authorized DoW, DAF, and ACC systems and personnel.

A2.1.7.3. **Analytic Production Stewards** are responsible for the data produced by their organization to ensure the dissemination, discoverability, accessibility, and interoperability by authorized DoW, DAF, and ACC personnel.

A2.1.8. **AI Stewards** are responsible for ensuring the ethical, responsible, and effective deployment of AI technologies within ACC, and are tasked with a variety of responsibilities that encompass governance, ethics, compliance, and the continuous improvement of AI systems.

A2.1.8.1. Manage AI systems to establish methods to oversee the quality, integrity, and security of the data used to train and operate AI models.

A2.1.8.2. Address biases and prioritize objectivity in AI algorithms.

A2.1.8.3. Ensure compliance with privacy regulations and ethical standards; promulgate and enforce ethical guidelines for the development and use of AI systems.

A2.1.8.4. Identify and mitigate AI associated risks, including cybersecurity threats and ethical dilemmas.

A2.1.8.5. Ensure the development, deployment, and use of AI in an ethical, transparent, and accountable manner, and assure AI solutions meet intended functions and deliver expected benefits.

## Attachment 3

## METADATA STANDARDS

**A3.1. Metadata.** Metadata is a key component to successfully provide meaningful context and quality data in a data-centric, zero-trust environment. It is necessary for search and discovery of data. Metadata provides attributes that enable access management with specific characteristics (e.g., person/nonperson entity). It empowers people and AI/ML tools to discover, correlate, and manage large sets of data across a distributed environment, thus enabling swift and appropriate decision making "more rapidly than adversaries are able to adapt."

**A3.2. Metadata Interoperability.** Metadata Interoperability is the ability for two or more systems or components to exchange descriptive data about things, and to interpret the descriptive data that has been exchanged consistently with a system-agnostic interpretation. Organizations will provide specific standards for metadata interoperability and tagging implementation, as specified by the DoD Metadata Guidance, to ensure seamless data exchange and integration across different systems and platforms.

**A3.3. Metadata Standards:**

A3.3.1. All data mandated by the Board must be appropriately tagged with the minimum metadata fields to ensure compliance with DoD minimum metadata standards.

A3.3.2. The metadata standards are listed in the DoD Metadata Guidance, available at **https://usaf.dps.mil/teams/CDAO/Public%20Repository/Forms/AllItems.aspx**