BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND

AIR COMBAT COMMAND MANUAL
14-422

24 OCTOBER 2023

Intelligence

INTELLIGENCE DATA GOVERNANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: ACC/A29D

Certified by: ACC/A2
(Col Abraham L. Jackson)
Pages: 17

This manual implements DAFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standards,* and AFI 90-7001, *Enterprise Data Sharing & Data Stewardship,* to provide prescriptive guidance for data governance. This ACCMAN applies to all Numbered Air Forces, Wings, Groups and Squadrons, at all levels that meets the following criteria: either, has a "responsibility to provide," intelligence data IAW Intelligence Community Directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information Within the Intelligence Community,* under U.S. Code, Title 50 and/or collect, produce, or disseminate Intelligence Data (as defined in this document) under U.S. Code, Title 10 authorities, including all civilian employees and uniformed members of the United States Air Force, and Air Force Reserve, Air Force Guard and those with a binding agreement or contractual obligation to abide by the terms of Department of the Air Force issuances or ACC issuances. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AFI 33-322, *Records Management and Information Governance Program,* and disposed of IAW the Air Force Records Information Management System Records Disposition Schedule. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Form 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-2, T-3") number following the compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures,* for a description of the authorities associated with the Tier numbers.

Chapter 1

GENERAL

1.1. Data Governance Overview. Data Governance ensures that data is managed as a critical enterprise asset consistent with ACC's mission enabling objectives. Data Governance is a discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, compliance, and enforcement), which together administer data and information assets. Data Governance focuses on the way decisions regarding data are made and how it is managed throughout its lifespan in order to accomplish mission outcomes, while ensuring access to the data at strategic, operational, and tactical levels. It confers control and authority over the data, thereby allowing mission-enabling functions to better leverage and extract value from data assets across the ACC Intelligence, Surveillance, and Reconnaissance (ISR) data enterprise. Data Governance is the foundation of Data Management and establishes policies, standards, guidance and higher-level procedures to ensure data is a functional enterprise asset; Data Management implements those policies, standards, guidance, higher-level procedures within Information Technologies (IT) platforms, systems, applications, and human 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. Some of the competencies/purposes of Data Governance are to:

1.1.1. Provide the principles, policies, processes, frameworks, capabilities/tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition.

1.1.2. Cultivate data stewardship practices across various levels within ACC.

1.1.3. Engage in organizational change management efforts that actively communicate to ACC's intelligence enterprise the benefits of managing data as a strategic enterprise asset.

1.1.4. Provide foundational oversight and technical baselines to:

1.1.4.1. Reduce or eliminate negative constraints to the discovery, use, and sharing associated with data that is tightly coupled to individual policies (unit, IT platform, systems, application and/or workflows).

1.1.4.2. Establish data and metadata commonality for automation, data fusion, and artificial intelligence/machine learning at scale by reducing the complexity and time associated with developing automation, fusion, and Artificial Intelligence/Machine Learning/Deep Learning (AI/ML/DL) using heterogenous data without a common baseline.

1.1.4.3. Allow intelligence analysts and warfighters to provide the AF and its mission partners the ability to leverage intelligence data to gain required operational efficiencies and tactical advantages.

1.2. Background. In the past, ACC intelligence data were tightly coupled with individualized Data Governance policies, frequently unit, IT platform, system, application, or workflow specific. This negatively constrained data discovery, use, and sharing processes across the enterprise. This critically impacted ACC intelligence enterprise's ability to incorporate vital information for time-

sensitive and mission-critical operations internally and for joint activities with other U.S. components or with our non-U.S. mission partners.

1.3. Purpose. This manual will further direct and guide the ACC intelligence enterprise in modernizing its Data Governance practices and implementations while aligning them with key mission partners. ACC intelligence data are strategic assets, and it is imperative that they are made discoverable, accessible, and usable at the speed of mission for AF, DoD, Intelligence Community (IC), Five-Eyes (FVEY) partners (Australia, Canada, New Zealand, United Kingdom and United States), and selected allies. This manual will:

1.3.1. Address Data Governance challenges for Airmen, processes, structures, and technologies.

1.3.2. Ensure technical implementation of Data Governance is aligned with IC, DoD, AF, and FVEY/Allied mission partners.

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 strong foundation for Data Governance.

1.4.1. **Leadership and Strategy:** Successful Data Governance depends on vision and committed leadership. ACC's intelligence vision and activities are informed by strategies provided by the AF, DoD, IC, and FVEY/Allies.

1.4.2. **Enterprise Driven:** Data Governance is an enterprise program, and as such, it must govern IT decisions related to data and enterprise interaction with data.

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 occurs at both the enterprise and local levels and all levels in between.

1.4.5. **Framework-based:** Because activities require coordination across functional areas, Data Governance must establish an operating framework that defines accountabilities and interactions.

1.4.6. **Principle-based:** Guiding principles are the foundation of Data Governance activities and must address multiple legal authorities.

Chapter 2

DATA GOVERNANCE BODIES

2.1. Managing Risk. To better manage risk, ACC will adopt a representative form of Data Governance, so all stakeholders have a voice and can be heard. Data Governance Bodies will be implemented to ensure consistency of intelligence data across ACC.

2.2. Disciplines. Data Governance and Data Stewardship disciplines facilitate the delivery of the right data to the right user at the right place and time. These bodies also function to inform decisions, shape a more data-driven culture based on feedback, and facilitate a collaborative ACC Intelligence data environment through consistent communication.

2.3. Framework. ACC's Intelligence Data Governance will be designed with the following bodies to ensure a successful framework is established.

2.3.1. **ACC Intelligence Data Governance Council (IDGC).** Will be chaired by ACC Intelligence Senior Data Office (ISDO); the IDGC is the primary and highest authority for ACC Intelligence Data Governance. The IDGC is responsible for the oversight and support of all ACC Intelligence Data Governance activities. The ACC IDGC will:

2.3.1.1. Consist of Executive Data Stewards (voting members), stakeholders, and subject matter experts across the ACC staff.

2.3.1.2. Publish a charter with defined scope, activities, and goals. Charter must be reviewed/updated annually or more frequently when deemed necessary.

2.3.1.3. Review NAF/Wing waivers and Plans of Actions and Milestones (POAM) and provide enterprise decision.

2.3.1.4. When applicable, request and secure funding for Data Governance and Data Governance sponsored activities recommended by, but not limited to: HHQ Data Governance Councils, DAF/CDAO, and/or the IC Chief Data and Artificial intelligence Office (CDAO).

2.3.1.5. Approve Data Governance policies and associated rules and procedures for implementation. Set a schedule for adoption of multi-intelligence discipline metadata standards.

2.3.1.6. Publish instructions and timelines for all units regarding documentation and compliance requirements mandated by this manual.

2.3.1.7. Manage Data Governance initiatives (e.g., development of policies, guidance, or metrics), issues, and escalations.

2.3.1.8. Serve as the final authority on disputes, such as disagreements between ACC organizations over data definitions and formats.

2.3.1.9. Create and direct necessary working groups with proper expertise in targeted subject areas related to Data Governance. The IDGC will assign a lead member responsible for the scheduling, planning, facilitating working group meetings, coordinating research, and reporting to the DGC.

2.3.1.9.1. Working groups will have well-defined goals and objectives to meet the intent of the IDGC. They will be temporary by nature and may provide guidance and advice on their specific areas of Data Governance.

2.3.2. **ACC Intelligence Data Governance Office (IDGO):** The IDGO will focus on enterprise-level intelligence data definitions and data management standards across all data management knowledge areas. The IDGO will:

2.3.2.1. Coordinate and define stewardship and data roles within the ACC Data Governance Program.

2.3.2.2. Provide applicable support to the governing bodies, data roles, working groups, and/or any organization under the ACC Data Governance program.

2.3.2.3. Maintain and publish all source documents related to Data Governance (e.g., data steward appointment letters, waivers, data standards, definitions, glossaries, policies, directives, models, domain ontologies, etc.).

2.3.3. **Data Stewardship Teams (DST):** Communities of interest focused on one or more specific subject-areas or projects, collaborating or consulting with project teams on data definitions and data management standards related to the focus. Consists of domain and technical data stewards and data analysts.

2.4. Intelligence Community Publications.

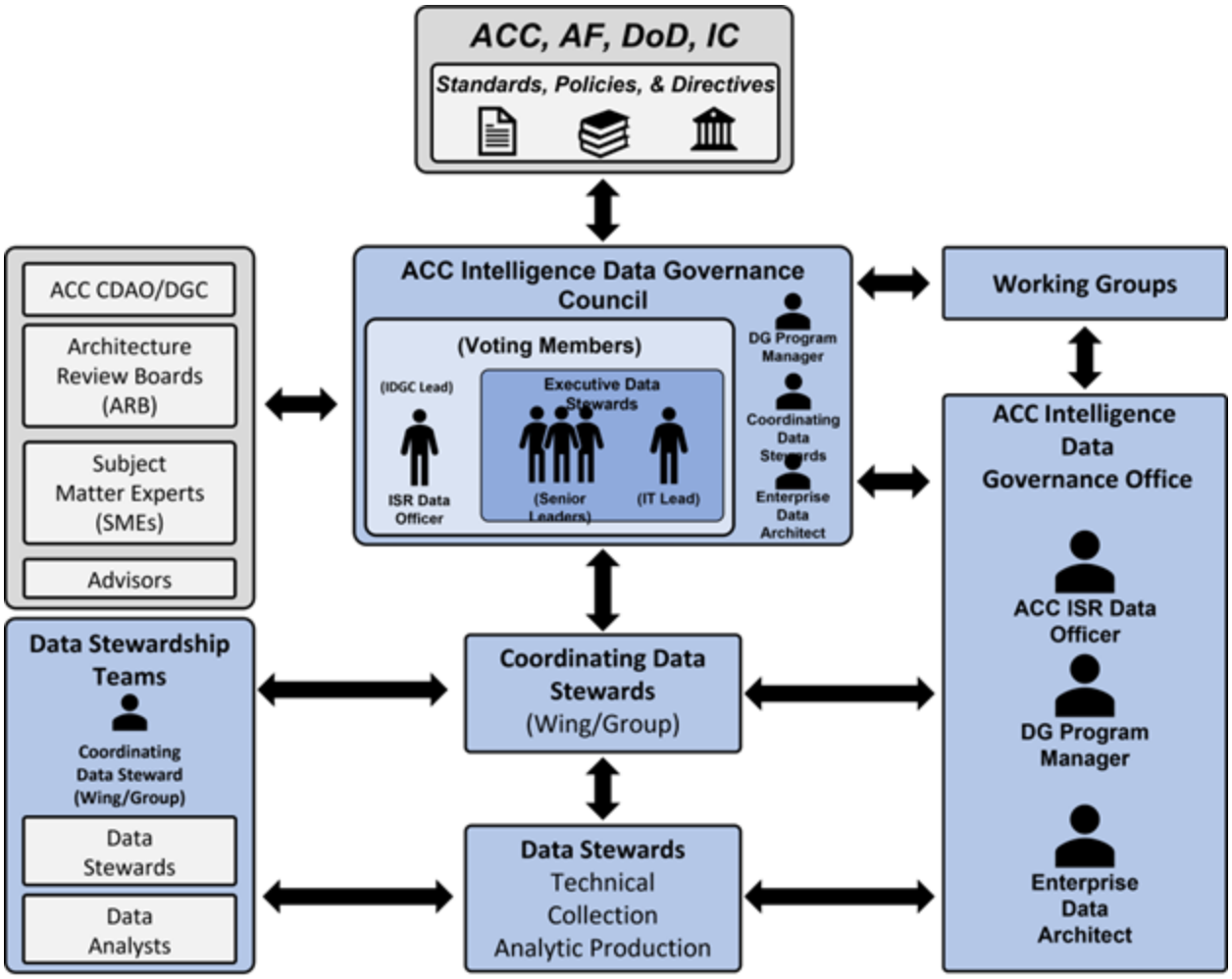
2.4.1. Intelligence Community Directive (ICD) Library: **https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives**.

2.4.2. Intelligence Community Policy Guidance (ICPG) Library: **https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance**.

2.4.3. Intelligence Community Policy Memorandums (ICPM) Library: **https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-memorandums**.

2.4.4. All attachments are located: **https://usaf.dps.mil/sites/haf-a2/A26O/ISREnterprisedatahub/MAJCOM%20Policy/ACC/ACCMAN%2014-422**.

Figure 2.1. ACC Intelligence Data Governance Bodies (Notional).



Chapter 3

ROLES AND RESPONSIBILITIES

3.1. Scope. This chapter outlines responsibilities for Intelligence data creation, storage, use, and dissemination by ACC/A2, assigned NAFs, and Wings.

3.2. Director of Intelligence (ACC/A2). ACC/A2 has overall responsibility for ACC Intelligence data and may delegate operational authority for ACC Intelligence Data Governance program to the ACC Intelligence Senior Data Officer (ISDO), ISR Data and Innovation Division Chief. ACC/A2's ability to govern data is derived from legal authorities vested in external entities which have delegated responsibilities to ACC/A2, to include Director of National Intelligence (DNI), Office of the Under Secretary of Defense for Intelligence (OUSDI), Headquarters Air Force (HAF) A2/6, and Commander, ACC (COMACC). Current IC, DoD, and AF reference documents may not be specific enough for unit-level implementation, ACC/A2 will direct the Intelligence Data Governance Council (IDGC) to develop and publish specific compliance, reporting, timeline and POAM/Waiver processes and requirements. The ISDO will provide updates quarterly to the ACC/A2 senior staff and others as directed.

3.3. ACC ISDO. ACC ISDO will establish and manage the ACC Intelligence Data Governance program in accordance with guidance from the ACC/A2. Additionally, the ACC ISDO will:

3.3.1. Ensure ACC Intelligence Data meets ACC, AF, DoD, and IC data policies, standards, guidance, and directives and represent ACC/A2 in higher-level forums or working groups as needed or directed.

3.3.2. Advise on tools and software capabilities to support Data Governance and Data Management.

3.3.3. Advise on data training, data literacy, human resources and organizational changes to support Data Governance and Data Management.

3.4. ACC Intelligence Data Governance Office (IDGO) will:

3.4.1. Advise and support the ACC ISDO in the management and execution of Data Governance and Data Management initiatives. See **Attachment 2.**

3.4.2. Coordinate with ACC A2 Training to establish minimum Data Stewardship training requirements.

3.5. ACC NAF, Wing, Group, and Squadron Commanders. Commanders will be responsible for ensuring their respective units are implementing all required Data Governance mandates, to include compliance with the requirements outlined in this manual in **paragraph 3.7**. Mandatory compliance with this document is based on whether a unit meets the following criteria: either, has a "responsibility to provide" intelligence data IAW ICD 501 under U.S. Code, Title 50 and/or collect, produce, or disseminate Intelligence Data (as defined in this document) under U.S. Code, Title 10 authorities, including all civilian employees and uniformed members of the United States Air Force, and Air Force Reserve, and those with a binding agreement or contractual obligation to abide by the terms of Department of the Air Force issuances or ACC issuances. ACC NAF, Wing, Group and Squadron Commanders who have not fully implemented higher AF, DoD and/or IC polices for Data Governance (i.e. visible, accessible, understandable, linked, trusted, interoperable

and secure) will adhere to IDGC published directions compliance, reporting, timelines, and POAM/Waiver processes and requirements.

3.5.1. Must appoint Intelligence Data Stewards, in writing, to ensure compliance with ACC's Intelligence Data Governance. **(T-3)** See **Attachment 2.**

3.5.2. May establish Data Steward Teams sufficient to meet Data Governance responsibilities. See **paragraph 3.6.1**.

3.5.3. May publish local Data Governance policies aligned and in compliance with higher level authorities.

3.5.4. Must use annual programming activities, site visits, and other means to highlight Data Governance resource shortfalls through their chain of command to ACC IDGC. **(T-3)**

3.6. Data Stewardship. Responsibilities will differ between the strategic, operational, and tactical levels as well as disciplines and mission functions. Intelligence Data Stewards may align to domains (**see Attachment 2**) at the strategic level, then further divide into categories at lower-level tiers.

3.6.1. **Data Stewardship Teams** are generally led by the senior-level Data Stewards at the organization. Generally, they consist of experts across a range of disciplines – operations, IT, data security, knowledge management, etc., but can be appointed from any Air Force Specialty Code (AFSC)/Civilian job series at the Commanders discretion. Teams focus on data governing and implementing Data Governance on the data within their organization's scope and responsibilities.

3.6.2. **Data Stewards Will:**

3.6.2.1. Adhere to guidance, policy, and directives published by the IDGC, support their Commander's Data Governance policies and implementation actions, and represent the Commander's equities in internal and external forums.

3.6.2.2. Complete the requisite training required to fill the role.

3.6.2.3. Manage assigned data sets as defined and determined by the IDGC and act with authority and accountability for management of assigned data within their purview.

3.6.2.4. Provide subject matter expertise in the context of mission execution and criteria for adhering to Data Governance policies including cataloging processes.

3.6.2.5. Ensure data under their area of responsibility is governed and cataloged.

3.6.2.6. Provide Data Governance and implementation feedback and recommendations through their chain of command and/or NAF/Wing level Data Governance Bodies.

3.6.2.7. **NAF and Wing Intelligence Data Stewards Will:**

3.6.2.7.1. Represent their NAF or Wing Data Governance working groups directed by ACC Intelligence Data Governance Bodies (designated Office of Primary responsibility).

3.6.2.7.2. Develop processes to ensure data tagging occurs in compliance with data standards mandated by the IDGC.

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

3.6.2.8.1. Adhere to higher level policies and processes to ensure data tagging in compliance with IC, DoD, AF, and/or with NAF/Wing.

3.7. ACC NAF/ Wing/Group/Squadron Commander's Compliance Requirements. (Templates for required documents listed below are located **https://usaf.dps.mil/sites/haf-a2/A26O/ISREnterprisedatahub/MAJCOM%20Policy/ACC/ACCMAN%2014-422**. If you have difficulty accessing this URL, please email the A29D organizational email box at: **ACCA2.A29D.Dataanlys@us.af.mil**).

3.7.1. Must comply with ACC, AF, DoD, and IC related instructions, policies, directives, publications, and Governance Bodies. **(T-3)**

3.7.2. Ensure Data Governance requirements are included in acquisition efforts.

3.7.3. Ensure minimum IC & DoD metadata standards listed, in **Attachment 3**, are met to ensure intelligence data is Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure (VAULTIS). **(T-3)**

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

3.7.5. Ensure participation in the appropriate Data Governance forums or working groups as directed by ACC Data Governance Bodies. **(T-3)**

3.7.6. Catalog all intelligence data at the lowest echelon while ensuring data is discoverable and shared beyond the unit. Cataloging is necessary to ensure compliance with this manual and to provide an accurate and up-to-date data inventory. Publicly Available Information (PAI) supporting intelligence operations will also be cataloged as required by existing guidance, policies, and/or directives. **(T-3)**

3.7.7. Identify priority datasets, considering the following data factors: criticality, sensitivity, quality, lineage, and regulatory requirements. Once priority datasets have been identified, governance policies and procedures can be established to ensure that data is managed effectively and efficiently.

3.7.8. Data Compliance Reports (DCR) provide commanders at all levels with a detailed compliance report into their Data Governance efforts. DCRs will identify all intelligence datasets under the commander's reporting authority, highlight datasets mandated by the IDGC, and identify responsible Data Stewards.

3.7.8.1. Additionally, DCRs will provide an overview for compliance requirements in their cataloging and tagging efforts and produced with the minimum information listed below unless directed otherwise by the ACC Intelligence Data Governance Bodies. **(T-3)**

3.7.8.1.1. Capture metrics totaling the number of known/managed/cataloged/curated data sets.

3.7.8.1.2. Identify needs, issues, and/or concerns requiring support from ACC Intelligence Data Governance Bodies.

3.7.8.1.3. NAF/A2 will survey, collect, and process non-ISR subordinate unit shortfalls for Intelligence Data Governance and forward to ACC IDGC for consideration and incorporations into strategic program plans.

3.7.8.2. **Quarterly:** Hold commander level internal DCR review.

3.7.8.3. **Annually** (February) or when requested by ACC Intelligence Data Governance Council:

3.7.8.3.1. Submit DCRs to the IDGO and the IDGC.

3.7.8.3.2. Complete and submit data maturity self-assessment results.

3.7.8.3.3. Complete and submit POAM when noncompliant with requirements outlined in this manual. POAM will include at a minimum: identified deficiencies, corrective actions, and timeline for unit compliance.

3.8. Authorized Intelligence Community Personnel (AICP) and Sensitive Review Board (SRB) members roles and responsibilities. AICP and SRB roles and responsibilities are established by ICD 501, *Discovery and Dissemination or Retrieval of Information Within the Intelligence Community*; Intelligence Community Policy Guidance (ICPG) 501.1, *Exception from Information Discovery,* and ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process*. These policies established intelligence data or information collected and analysis produced under Title 50 authorities as national assets. As such, intelligence professionals shall act as stewards of information having a predominant "responsibility to provide" intelligence information. In addition, authorized IC personnel have a "responsibility to discover" intelligence information believed to have the potential to contribute to their assigned mission need and a corresponding "responsibility to request" relevant intelligence information they have discovered. This manual is designed to supplement AICP and Data Sharing Regulation Board member's roles and responsibilities. If there is a conflict, the conflict will be elevated to the ACC/A2 DGC for final resolution.

MARK D. KELLY, GENERAL, USAF
COMMANDER
AIR COMBAT COMMAND

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

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

DAFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft/Data Standards*, 26 May 2021

DAFMAN 90-161, *Publishing Processes and Procedures*, 15 April 2022

ICD 501, *Discovery and Dissemination or Retrieval of Information Within the Intelligence Community*, 21 January 2009

ICPG 501.1, *Exemption of Information from Discovery*, 26 May 2009

ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process,* 26 May 2009

JP 2-0, *Joint Intelligence*, 26 May 2022

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

5EE—Five Eyes Enterprise

AFSC—Air Force Specialty Code

AICP—Authorized Intelligence Community Personnel

AI/ML/DL—Artificial Intelligence and Machine Learning and Deep Learning

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

DOD CDAO—Department of Defense Chief Digital and Artificial Intelligence Office

DNI—Director of National Intelligence

FVEY—Five-Eyes

HAF—Headquarters Air Force

HHQ—Higher Headquarters

IC—Intelligence Community

ICPG—Intelligence Community Policy Guidance

IDGC—Intelligence Data Governance Council

IDGO—Intelligence Data Governance Office

ISDO—Intelligence Senior Data Office

ISR—Intelligence, Surveillance, and Reconnaissance

IT—Information Technology

NAF—Numbered Air Forces

OUSDI—Office of the Under Secretary of Defense for Intelligence

PAI—Publicly Available Information

POAM—Plan of Action & Milestones

SRB—Sensitive Review Board

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

Terms

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 Data Management Lexicon)

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

Chief Data Officer—A designated Senior Official within each IC Element 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 Data Management Lexicon)

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 Data Management Lexicon)

Data as an IC Asset—Data that may be relevant to one or more IC elements for intelligence purposes. (Source: IC Data Management Lexicon)

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 Data Management Lexicon)

Data Governance—A discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, conformance, and enforcement), which together administer data and information assets across an IC Element to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives. (Source: IC Data Management Lexicon)

Data Governance Council—A decision making and/or policy making council of senior managers, chaired by the CDO, who are responsible for the highest tier of data governance in an IC Element. The Data Governance Council (DGC) oversees or manages data governance initiatives (e.g., development of policies or metrics), issues and escalations. The DGC monitors

results to ensure the IC elements receive the desired outcomes and business value from data management activities. This may also be called a Data Council, Executive Data Council or Data Executive Council. (Source: IC Data Management Lexicon)

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 Data Management Lexicon)

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

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 Data Management Lexicon)

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 Data Management Lexicon)

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 Data Management Lexicon)

Master Data—Core mission and business data entities used in traditional or analytical applications across an organization, and subjected to enterprise governance policies, along with their associated metadata, attributes, definitions, roles, connections and taxonomies. Master data provides context for mission and business activity data in the form of common and abstract concepts related to activity transactions, along with consistent and uniform set of identifiers and extended attributes that describe the core entities. (Source: IC Data Management Lexicon)

Master Data Management—Processes that control management of master data values to enable consistent, shared, contextual use across applications, of the most accurate, timely, and relevant version of truth about essential mission and business entities. Usually enabled by technology so that mission, business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official shared master data assets. (Source: IC Data Management Lexicon)

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

Mission Data—Data gathered, acquired, generated, held, or obtained during mission activities by an organization (e.g., IC element, DoD 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 Data Management Lexicon)

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 Data Management Lexicon)

Intelligence—1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations conducting such activities. (Source: JP 2-0)

Intelligence, Surveillance, and Reconnaissance—1. An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. 2. The organizations or assets conducting such activities. (Source: JP 2-0)

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.

ISR Data—Refers to the information collected through intelligence, surveillance, and reconnaissance activities. It focuses on the data obtained from direct sources, sensors, cameras, and other intelligence-gathering technologies used to provide situational awareness and support decision-making processes. ISR Data can include imagery, video, audio, and signals intelligence (SIGINT) data collected from various platforms such as satellites, aircraft, drones, ground-based sensors, and other surveillance systems. ISR data is a subset of intelligence data and is used to generate intelligence products and support military operations.

Attachment 2

POTENTIAL DATA STEWARDSHIP ROLES

A2.1. Data Stewardship. Data Stewardship is the most common label to describe accountability and responsibility for data processes that ensure effective control and use of data assets.

A2.2. Types of Data Stewards:

A2.2.1. **Chief Data Stewards** leads Data Governance Offices and chairs Data Governance Councils. Participates in higher level Data Governance Bodies to ensure compliance of upper-level policies, standards, guidance, and directives.

A2.2.2. **Executive Data Stewards** are senior leaders with voting power who serve on Data Governance Councils and include an IT Lead.

A2.2.3. **Domain Data Stewards** have oversight of a specific data domain within an enterprise (e.g. INT-Specific, CCMDs, Platforms, etc...).

A2.2.4. **Coordinating Data Stewards** lead and represent Data Steward Teams under their organizational structure. Normally reside at the wing & group levels.

A2.2.5. **Data Managers** are members who assume approval authority for decisions about data within their domain.

A2.2.6. **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.

A2.2.6.1. **Technical Data Stewards** are often IT professionals that provide the technical expertise around source systems, Extract, Transform, and Load (ETL) processes, data stores, data warehouses, and business intelligence tools. Technical Data Stewards produce/maintain data flow schema & mapping of data within their organization.

A2.2.6.2. **Collection Stewards** are responsible for the collected intelligence data to ensure the dissemination, discoverability, accessibility, and interoperability by authorized ACC, AF, DoD, and IC systems and personnel.

A2.2.6.3. **Analytic Production Stewards** are responsible for the intelligence data produced by their organization to ensure the dissemination, discoverability, accessibility, and interoperability by authorized ACC, AF, DoD, and IC systems and personnel.

Attachment 3

METADATA STANDARDS

A3.1. Metadata. Metadata is a key component to successfully provide meaningful context and quality to 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/DL 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 implement metadata tags to achieve interoperability as specified in the guidance table.

A3.3. Metadata Standards:

A3.3.1. All data mandated by the IDGC must be appropriately tagged with the minimum metadata fields to ensure compliance with 5EE Enterprise Data Headers and IC mandated intelligence discipline specific metadata standards.

A3.3.2. DoD Metadata Guidance (**https://usaf.dps.mil/sites/haf-a2/A26O/ISREnterprisedatahub/Policy%20Catalog/dod%20metadata%20guidance.pdf**)