CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-9010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
(ATTN: CHIEF INFORMATION OFFICERS, CHIEF DATA OFFICERS)
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
(ATTN: DIRECTOR OF COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS/CYBER J6)
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
(ATTN: CHIEF INFORMATION OFFICERS, CHIEF DATA OFFICERS)
DIRECTORS OF DEFENSE AGENCIES
(ATTN: CHIEF INFORMATION OFFICERS, CHIEF DATA OFFICER)
DIRECTORS OF DOD FIELD ACTIVITIES
(ATTN: CHIEF INFORMATION OFFICERS, CHIEF DATA OFFICERS)

SUBJECT: Department of Defense Metadata Guidance

The enclosed metadata guidance consolidates and clarifies existing policy and requirements from a variety of Department of Defense (DoD) and Federal sources. Clear and consistent metadata management underpins the secure, interoperable data environments needed for decision advantage and is essential for implementing the DoD Data Decrees, DoD Data Strategy, and DoD Digital Modernization Strategy. Metadata management also supports data practitioners throughout the Military Departments, Combatant Commands, Defense Agencies, and Field Activities as they build data-centric, zero-trust environments across the enterprise.

Generating and applying metadata consistent with the enclosed guidance aligns with the DoD Data Strategy and foundational interagency specifications. In addition, cataloging and publishing metadata will bring valued insights to data consumers and supports data interoperability across DoD environments. A data asset will acquire metadata, whether mission or functional, throughout its lifecycle. The enclosed guidance outlines a baseline of minimum metadata to be applied initially. As data is shared, additional metadata may be applied.

Implementation of this guidance in the Department with significant technical debt will not occur overnight; however, we must start on the journey and identify any barriers in the way of achieving our ability to be a data-centric organization. The Chief Digital and Artificial Intelligence Office (CDAO), as the advocate for this guidance, is interested in component feedback on implementation best practices and systemic blockers. The CDAO will actively seek to remove barriers to implementation, using the CDAO Council as the forum to align and accelerate our application of metadata.

To that end, my team is available to answer any questions and provide assistance as needed. The team can be reached via email at osd.pentagon.cdao.mbx.cdao-council-exec-sec@mail.mil.

MARTELL.CRAIG.HARRY.1269768998

Digitally signed by MARTELL.CRAIG.HARRY.1269768998
Date: 2023.03.13 15:25:35 -07'00'

Dr. Craig H. Martell

Enclosure:
DoD Metadata Guidance

Department of Defense

Chief Digital and Artificial Intelligence Officer

DoD Metadata Guidance

Version 1.0

January 2023

Table of Contents

Table of Contents

1 Executive Summary

This metadata guidance aligns to the 2020 DoD Data Strategy, DoD and Federal regulations, and identifies ten metadata requirements that promote data visibility. These ten requirements are intended as an initial common baseline, and are not intended to be all encompassing. Metadata should be applied to a data asset at the most appropriate time between creation and storage. A DoD organization may add more than the minimum amount of metadata, and it may not be appropriate to apply all the metadata simultaneously. When applied appropriately and correctly, metadata aides mission success. However, if applied inappropriately and incorrectly it can be both a hindrance and a burden. This guidance was derived from the U.S. Federal Government metadata requirements published in Priority Objective #3 (PO#3) as well as North Atlantic Treaty Organization (NATO) and National Archive and Records Administration (NARA) metadata requirements. This common baseline is intended to provide a consistent starting point for any type of source of DoD data, such as Warfighting, Intelligence, or Business.

2 Introduction

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/non-person entity). It empowers people and artificial intelligence (AI)/machine learning 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." (2020 DoD Data Strategy, cleared for public release, para. 3. ESSENTIAL CAPABILITIES, found at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF).

The Deputy Secretary of Defense (DSD) memorandum, "Creating Data Advantage", dated May 5, 2021, provides five data decrees – summarized as: maximize data sharing and rights; publish data assets; automate data interfaces; store data uncoupled from hardware and software dependencies; implement industry best practices to secure data[1]. This metadata baseline is aligned to the Data Decrees, as well as the DoD Data Strategy and the Digital Modernization Strategy. The DoD Chief Data Officer (CDO), published the DoD Data Stewardship Memorandum and Guidebook on October 24, 2021. The guide provides CDO, Data Steward, and Data Custodian roles and responsibilities. This guidance along with the DSD "Creating Data Advantage" memorandum dated May 5, 2021, directs DoD Components to coordinate their data activities by establishing appointed data leaders (e.g., CDOs, data stewards). The application of metadata is part of the DoD Data Stewardship roles and responsibilities.

This guidance provides insight into the 10 DoD metadata baseline requirements, such as 6 basic metadata functional areas and how to apply additional mission specific metadata. This guidance also provides recommendations and requirements to baseline disparate, existing metadata requirements. This guidance does not provide specific implementation instruction or metadata technical patterns including standardization of metadata tagging (the actual implementation of the metadata). There are various standards available for the DoD that address metadata requirements and strategy. Selection of the approach and standards is based on operational and technical needs, and should be accomplished in a way that minimizes operational burdens, such as through the use of automation. Implementation and metadata must be in compliance with and executed in accordance with existing DoD and Federal policies and regulations, such as Privacy and Civil Liberties, Information Security, Cybersecurity, Intelligence Oversight, Human Research Subject Protection, Records Management, Acquisition and Procurement (including Agreements and Other Transaction Authority), Fiscal, and including the DoD Responsible Artificial Intelligence Strategy and Implementation Pathway. In some instances, specific policies or regulations dictate specific metadata information content and provide guidance for both DoD data producers and consumers.

[1] DoD Data Decrees in full. "To generate the transformative proficiency and efficiency gains across the DoD Data Strategy' s focus areas of Joint All Domain Operations, Senior Leader Decision Support, and Executive Analytics, the Department will apply the following five 'DoD Data Decrees': 1. Maximize data sharing and rights for data use: all DoD data is an enterprise resource. 2. Publish data assets in the DoD federated data catalog along with common interface specifications. 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. 4. Store data in a manner that is platform and environment-agnostic, uncoupled from hardware or software dependencies. 5. Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use." (DSD Memorandum of May 5, 2021, found at https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF).

2.1 Importance

With the department's focus on data, there has been and will continue to be a need to become a data-centric environment. However, there is no DoD guidance regarding what metadata should be used and how it should be applied to the data assets. Establishing a baseline minimum set of metadata and applying it as soon as is appropriate between the time of creation and the time of storage supports the DoD's foundational data needs without placing an unnecessary load on the communication systems that need to transport information in what may be a highly contested environment. Without a common baseline, every community of interest or organization will apply metadata in a different way, which makes department-wide interoperability challenging and drives the usage of complex or error-prone mapping to achieve the DoD Data Strategy Goals[2]. It is therefore necessary to establish a unified and common pattern for metadata creation to enable enterprise interoperability. Defining a limited set of metadata necessary for any DoD data to support foundational data functionality within the DoD will provide the common starting point to create and apply metadata.

2.2 Scope and Applicability

Metadata shall be applied to a data asset at the most appropriate time between creation and storage (also referred to as application, implementation, or use), but not later than the time of storage, and shall be executed in a way that does not jeopardize mission success while in compliance with DoD and Federal regulations. This covers any data in accordance with DoD policy generated on behalf of or in support of DoD operational, intelligence, or business activities (e.g., Warfighter, Intelligence, Business, and Enterprise Information Mission Areas). Additional areas of opportunity include structured or unstructured data such as, machine to machine data (sensor data, track data, etc.), geospatial information, personnel and medical records, financial data, AI artifacts, videos, binary, query search results, databases, data sets, containers, proprietary/non-proprietary etc. Every data asset should include mission relevant metadata. Metadata elements are populated throughout the information lifecycle. Communities of Interest will leverage community specific metadata when applicable. The Data Steward/Data producer should ensure that the mission metadata can be applied as efficiently as reasonable/possible. Data assets metadata policy is under authority of the Chief Digital and Artificial Intelligence Officer (CDAO). Infrastructure and applications metadata policy is under the DoD Chief Information Officer (DoD CIO) authority.

The most appropriate time for applying metadata may vary between the time of creation (the birth of a data asset prior to the first exchange) and storage (uploading to shared memory where other entities may search for and retrieve the data). The application of different metadata fields may also vary with time. For example, the time and date created may be applied at inception of the data asset, while the Custodian may be applied when the data is first stored in a shared database.

Applying metadata means the metadata is associated with, and in some instances physically located with, the data - for example, as in a data store. The metadata may reside in a different location from the data asset such as a metadata catalog. The minimum metadata and other mission specific metadata are a permanent feature of data and exists if the data asset exists. When data is exchanged

2 VAULTIS visible, accessible, understandable, linked, trustworthy, interoperable, and secure.

in a machine-to-machine message the metadata may be discarded (see Figure 1).

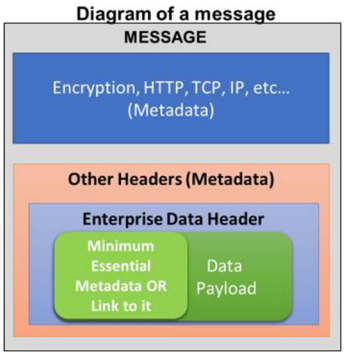

Figure 1. As data assets are shared, only critical metadata should travel in the payload (e.g., ID and date/time).

Care must be taken in how much metadata travels in the payload of the message. It is critical to optimize for efficiency of transport when dealing with data in motion, such as from a sensor to a shooter. This efficiency is achieved through compact, efficient, trustworthy, interoperable, and secure (CETIS) goals. Failure to adhere to the CETIS goals may lead to mission failure in a highly contested environment. In support of the CETIS goals, only the mission-critical pieces of critical metadata (e.g. identification (ID) and Data/Time) should be included in the payload. The full complement (provenance and lineage) of metadata can be retrieved using the ID and the date/time from a catalog when needed.

2.3 Assumptions

The following assumptions apply to the content in this document:

a) All organizations across DoD will apply the DoD Metadata Guidance.
b) Data Stewards within an organization or community will apply metadata at the most appropriate time between creation and storage and maintain the tagging throughout the data assets' life cycles within their domain.
c) Metadata (functional or mission-specific metadata) will be accessible via the DoD Federated Data Catalog hosted in the CDAO's Advana platform.
d) The Department will implement/tag their data using various tools (e.g., an IT service) available for the enterprise, as a local service, or inherent in a material capability.
e) All metadata will be created aligned to the DoD Strategy goals.
f) This metadata guidance does not supersede existing policy. Satisfying these principles will be executed in accordance with all appropriate Federal, DoD, and International policies, regulations, and agreements.

3 Guidance

During the latter part of 2020 and throughout 2021, the DoD CDO and Joint Staff (JS) J6 held a series of Metadata Workshops. The workshop membership included members from the Services, Combatant Commands, other Joint Staff directorates, DoD CIO, Intelligence Organizations, and Coalition partners. During these workshops, the members established the minimum metadata by drawing from various documents published by U.S. Federal Government, to include National Archive and Records Administration (NARA) Code of Federal Regulations, as well as the international community. Members identified data enrichment opportunities through the development of two key products – a list of basic metadata functions, and the minimum metadata supporting those functions. Sections 3.1 through 3.4 provide the DoD metadata functional areas and selection criteria established, as well as the key documentation used to develop metadata best practices. Guidance for functional area considerations stem from U.S. PM-ISE PO3, v1 and Intelligence Community Data Lexicon.

3.1 Functional Area Considerations

Applying metadata will promote data quality and mission-focused insights. The Joint Staff identified six functional areas, which include: search and discovery, access control, correlation, audit, records management, and protection. Below are the definitions of these functional areas:

a) Search & Discovery: The ability to locate and obtain knowledge of the existence of, but not necessarily the contents of, a resource. (U.S. PM-ISE PO3, v1 – Data Tagging Functional Requirements)
b) Access Control: Granting or denying specific requests for resources based on a defined set of criteria. (U.S. PM-ISE PO3, v1 – Data Tagging Functional Requirements)
c) Correlation: Identifying relationships between entities within and across disparate data sets. (U.S. PM-ISE PO3, v1 – Data Tagging Functional Requirements)
d) Audit: Recording the sequence of actions surrounding or leading up to a specific activity or event. (U.S. PM-ISE PO3, v1 – Data Tagging Functional Requirements)
e) Records Management: Managerial activities involved with the creation, update, retention, and disposition of records. Records Management provides life cycle management within DoD. (U.S. PM-ISE PO3, v1 – Data Tagging Functional Requirements)
f) Protection: Processes, services, and methods used to accomplish the privacy, safety, confidentiality, integrity, availability and recovery of data. (IC Data Lexicon, January 2020)

3.2 Functional Area Use Cases

Below are the JS provided use cases illustrating how functional areas could be applied within the ecosystem. Each use case provides a scenario to a functional requirement, an outcome, and metadata function. The specific use cases are focused on discovery, access, and protection to demonstrate the functionality of incorporating metadata.

Search & Discovery. All metadata fields support this function.

Scenario: The DoD has received a Freedom of Information Act (FOIA) request for all unclassified information about an incident that occurred on a military installation in the U.S. Within 20 business days, the Department is required to determine whether to comply with the request. The disclosure of documents is required to follow promptly thereafter. All data handled by the Department is appropriately tagged with the minimum enterprise metadata. Utilizing the Department's enterprise search capability, a query is made throughout the federated data catalog.

Outcome: The system quickly returns unclassified metadata on documents based upon the query's criteria. Human review is conducted, and documents are disclosed in accordance with applicable law, policy, and regulation.

Metadata Function: The metadata allowed the system to quickly differentiate thousands of documents based upon criteria entered in the Department's enterprise search capability, identifying the relevant unclassified documents related to the incident.

Access Control. The metadata fields supporting this function include: Security Classification, Disclosure & Releasability, Handling Restrictions, and Format to physically access the data required.

Scenario: A combatant command wants to share data with appropriately authorized foreign government mission partners in an environment where multiple mission partners are authorized access, but specific missions are restricted based on mission assignment/membership denoted by a tetragraph. The U.S. originated data is labeled "REL to USA, TETR", where "TETR" is a recognized tetragraph representing an authorized mission partner coalition. Labeling the data with "REL to USA, TETR" implements the sharing/safeguarding of the data and allows the access control system to determine if person and non-person entity systems and applications are members of mission TETR, and if they are authorized access.

Outcome: The attribute-based access control system evaluates whether the entities requesting access are members of mission TETR, and grants or denies access to the resource.

Metadata Function: The metadata allowed the access control system to identify the resource as releasable to coalition partners in mission group TETR.

Correlation. The metadata fields supporting this function include: DataItemCreateDateTime and Description.

Scenario: An analyst is reviewing sensor observation data for processing and the application of AI algorithms with other intelligence data to determine if there are linkages between persons of interest and ongoing operational activities. The analyst is consolidating the package which includes mission-based attributes. The algorithm results indicate a relationship between a particular sub-set of activities and a specific person of interest. The analyst shares AI-derived results and the corresponding sub-set of data with other analysts to validate the results.

Outcome: The AI-enabled results lead to recommended changes in ground operations in order to deter the adversary.

Metadata Functions: The metadata (description and DataItemCreateDateTime) along with mission specific metadata allowed the capability to discover the correlation or linkage between different data sets. The Identifier allowed the primary analyst to effectively share the sub-set of data with colleagues.

Audit. The metadata fields supporting this function include: Identifier, Originator, Description, and DataItemCreateDateTime.

Scenario: An operational cell using a senior leader dashboard notices information discrepancies, specifically, if the dashboard is missing key information previously reported. The cell operators submit a dashboard trouble ticket. An audit of the missing information identifies data quality issues with the dashboard data feeds. The dashboard managers provide the Data Stewards of the source data the specific missing information using the metadata.

Outcome: The Data Stewards rectify the missing data. Dashboard reflects updated information.

Metadata Functions: The metadata provided the dashboard managers the mechanism to identify the specific missing data and communicate that to the Data Stewards for action.

Records Management. The metadata fields supporting this function include: Description, Format, Custodian, Security Classification, Disclosure & Releasability, and Handling Restrictions.

Scenario: The DoD has received a FOIA request for all unclassified information about an incident that occurred on a military installation in the U.S. Within 20 business days, the Department is required to determine whether to comply with the request. The disclosure of documents is required to follow promptly thereafter. All data handled by the Department is appropriately tagged with metadata. The FOIA request is tasked to the Custodian that is responsible for records from the military installation. Utilizing the Departments enterprise search capability, a query is made throughout the federated data catalog.

Outcome: The system quickly returns documents based upon the query's criteria. Human review is conducted and any follow-up issues are resolved with the Custodian identified in the responsive data. Documents are disclosed IAW applicable law, policy, and regulation, and the FOIA request, and results are tagged with in the appropriate data asset.

Metadata Functions: The metadata allowed the task to be assigned automatically to the legally responsible office. The metadata allowed the system to quickly differentiate thousands of documents based upon criteria entered in the Departments enterprise search capability. The metadata provided a reference for any follow up concerns or issues.

Protection. The metadata fields supporting this function include: Identifier, Data & Time Created, Description, Format, Security Classification, Disclosure & Releasability, and Handling Restrictions

Scenario: Command X monitors data access. An algorithm detects anomalous activity - a large

volume of data accessed by an authorized entity that historically does not access that volume of data. Command X continually tracks the accessed data using the metadata while determining if the anomalous activity is warranted. Command X determines the volume of data access was not justified by the entity, shuts down that entity's access, and 'retrieves' the data.

Outcome: The Command quickly tracked and retrieved mishandled data reducing the risk and exposure, as well as the level of effort and time to 'clean' the various environment(s) the data flowed through.

Metadata Function: The metadata allowed the command tools to track and retrieve the specific data rather than combing through multiple systems, databases, and environments to determine where the data flowed.

3.3 References

In order to select a DoD minimum set of metadata, the CDO and JS J6 writing team reviewed existing, applicable metadata documentation. The result was an extensive range of code, policy and standards. Most of these publications based their metadata requirements on the Dublin Core[4]. Ultimately, seven publications played a significant role in determining the metadata context. Below is the list of the five specific resources consulted.

An amalgamation of the NARA Code of Federal Regulations, the NARA Bulletin, and the Universal Electronic Records Management Requirements comprise the NARA metadata requirements included in Appendix D.

a) Program Management – Information Sharing Environment (PM-ISE) Priority Objective 3 (PO3), v1 – Data Tagging Functional Requirements, Dec 2014. This is the U.S. Federal Government's published metadata requirements.
b) NARA Code of Federal Regulations Subchapter B – Records Management, chapter XII of Title 36, Code of Federal Regulations (36 CFR 1236.12)
c) Title 44, United States Code.
d) NARA Bulletin 2015-04: Metadata Guidance.
e) Universal Electronic Records Management Requirements, v2 developed by the NARA Requirements Working Group.
https://www.archives.gov/records-mgmt/policy/universalermrequirements
f) NATO Core Metadata Specification, STANAG 5636.
g) DoD Instruction (DoDI) 5015.02, DoD Records Management Program, found at https://www.esd.whs.mil/Directives/issuances/dodi/

3.4 Metadata

Below are the 10 baseline required metadata fields that shall be applied at the most appropriate time between creation, but not later than the time of storage. Any organization can apply more than the minimum identified metadata fields. The metadata fields are broken into two categories: Resource Description and Safeguarding and Sharing (Entitlements Management). The requirement provides the metadata title, definition, and further decomposition of the definition as

well as some amplifying information. There are some metadata information that should never change throughout a data asset's lifecycle. However, if an error occurs in this type of metadata, it should be corrected. There are various mechanisms available to correct an error and still preserve the metadata lineage and provenance. It is out of scope for this document to outline these mechanisms but should be addressed in future work.

Metadata Field Description

Identifier[3] - A universal, unambiguous (unique) reference to the resource (Modified PO#3, NARA, and NATO). Decomposition: A data asset has only one Globally Unique Identifier (GUID) throughout its life cycle, but may have more than one domain specific identifier assigned during its life cycle. For example, a data asset has its GUID, but could also have a domain specific identifier. The GUID should be consistent (standardized) within and across domains. It supports identification of the data asset but should not give away information about the data asset. The universally unique identifier should never change throughout the life cycle of a data asset.

Authorization Reference[4] - The particular documented legal basis for mission activities associated with the creation, retention and use of a resource (PO#3). Decomposition: This is any document that provides the authority to act on or manage the data asset. Authority should be as specific as possible. A data asset may have different authorities over time. Potential types of Authorization Reference documents include: U.S. Law, Regulation or Government-wide Policy; DoD Execution Operational Orders (U.S. or Coalition OPORD); DoD Policy; DoD Memorandum; Memorandums of Agreement, Memorandums of Understanding, Specific DoD Organization policy; Court Order; Fragmentation Orders (U.S. and Coalition FRAGO); Bi-lateral Agreements; and other appropriate Coalition/Multinational agreements, etc.

Originator[5] - An entity (organization) primarily responsible for generating the resource. For DoD, "Originator" is synonymous with author, producer, creator, and collector. (PO#3, NARA, and NATO). Decomposition: This metadata field is an organization (e.g., Command, Operational Cell). It could also include an organizational role or position as well as a person or non-person entity. This field may have multiple applicable fields. The Originator organization should not change throughout the data asset life cycle.

Custodian[6] - The organizational element that is legally responsible for making decisions related to the data asset (e.g., records management, declassification, eDiscovery, FOIA search) (modified from NARA), in DoD designated as data steward. Decomposition: There are legal mandates for all data at the time of creation and throughout the data lifecycle. All data must be properly managed from creation to disposition. The Custodian organization is responsible for ensuring that legal needs data requirements are satisfied by actively applying the required management

3 Supplemental information for Identifier can be found: XML Data Encoding Specification for Intelligence Community Enterprise Data Header (EDH) v 2019 March

4 Supplemental information for Authorization Reference can be found: XML Data Encoding Specification for Intelligence Community Enterprise Data Header (EDH) v 2019 March

5 Supplemental information for Originator can be found: XML Data Encoding Specification for Intelligence Community Enterprise Data Header (EDH) v 2019 March

6 Supplemental information for Custodian can be found: XML Data Encoding Specification for Intelligence Community Enterprise Data Header (EDH) v 2019 March

practices. This metadata requirement is an organization (e.g., Command, Operational Cell) but may also include a person, position or role. The Custodian organization may be the same organization as the Originator or they can be different organizations. The Custodian organization can change during the data asset's lifecycle.

DataItemCreateDateTime[7] **-** Date and time on which the data resource was created to include when a data resource came under government control (i.e., acquisition of third party data, etc.) (modified from NATO). Decomposition: This metadata covers year, month, day, and time a data asset is created represented by Universal Time Coordinated (UTC). Date and time created also represents the first instance a data asset is acquired (e.g., Publically Available Information) by DoD and appears in the DoD IT environment. The date and time created should never change throughout the data asset's life cycle.

Description - Provides an overview of the contents of the asset (e.g., Summary, Abstract, Table of Contents). (PO#3, NARA, and NATO). Decomposition: The description should provide a brief description of the data asset's original purpose, which provides context. This is a free text abstract. It may contain any relevant information that supports the original purpose of the data asset at the time of creation. It may contain information on the how the data was created and any limitations or constraints. It is important to note that a data asset maybe used for other purposes beyond the original purpose and may obtain additional description metadata to address those additional uses.

Format[8] - Information about the file format, physical medium, or dimensions of the resource. (NATO). Decomposition: The physical attributes of the data asset, for example, the format type (e.g., email, JPEG). Format metadata information is important for machine to machine interoperability as well as human consumption. Size is another example of a physical attribute of a data asset. Size is supplemental format information.

Safeguarding & Sharing (Entitlements Management)

Security Classification[9] – An indicator identifying the highest level of classification contained within a resource (NARA and NATO). Decomposition: This metadata information provides classification and the reference used to determine the classification (e.g., Policy, Security Classification Guide. In addition, this metadata requirement covers multiple content fields such as the Special Access Programs, Classifier (organization and/or person), Originating Classification Authority, Retention, Derivative Classification Authority, etc. Originating Classification requires four lines (Originator, Reason(s), Downgrade On, Declassify On) of metadata in addition to the level of classification. All organizations must follow DoD and/or NATO policy regarding the classification rules regulating the values used to satisfy this requirement. E.g., refer to DoDM 5200.01, DoD Information Security Program (Volumes 1, 2 (Marking of Information), and 3).

Disclosure & Releasability[10] **-** Information pertaining to countries, organizations, or communities

7 Supplemental information for DateItemCreateDate can be found: XML Data Encoding Specification for Intelligence Community Enterprise Data Header (EDH) v 2019 March

8 Supplemental information for Format can be found: NATO Core Metadata

9 Supplemental information for Security Classification can be found: XML Data Encoding Specification for Information Security Markings v 2016-Sep2017-Jul

10 Supplemental information for Disclosure & Releasability can be found: XML Data Encoding Specification for Information Security Markings v 2016-Sep2017-Jul

approved to receive the resource (PO#3, NARA, and NATO). Decomposition: This metadata requirement requires at least one of these categories: Country/Countries, Recognized Organization or Community (e.g., NATO, FVEYs, etc.), or a group/category of people (e.g., contractors, government, foreign personnel, public) and their access rights. The data asset metadata may contain all three categories. All organizations must follow DoD and/or NATO policy regarding the disclosure and releasability rules regulating the values used to satisfy this requirement. E.g., see also DoDM 5200.01, DoD Information Security Program (Volumes 1, 2 (Marking of Information), and 3); DoDI 5230.09, Clearance of DoD Information for Public Release; and, DoDI 5230.29, Security and Policy Review of DoD Information for Public Release.

Handling Restrictions[11] **-** Limitations not related to classification or releasability, such as Controlled Unclassified Information designations. (PO#3 and NARA). Decomposition: This metadata covers such content as privacy controls, specific purpose, use limitations, authority (e.g., legislation, policy), personally identifiable information, law enforcement restrictions, medical restrictions (e.g., Individual Identifiable Health Information, Health Insurance Portability and Accountability), and licensing. Indicating no special handling restrictions is also valuable. It alerts the consumer that handling restrictions were considered. All organizations must follow DoD and/or NATO policy regarding the handling restrictions regulating the values used to satisfy this requirement. E.g., refer to DoDI 5400.1, DoD Privacy and Civil Liberties Programs.

11 Supplemental information for Handling Restrictions can be found: XML Data Encoding Specification for Information Security Markings v 2016-Sep2017-Jul

4 Metadata Application

The CDOs and Data Stewards must work with Community of Interest (CoI) operational subject matters experts (SMEs), program managers, system developers, and records managers, to develop and manage their community functional or mission specific metadata processes. Once they have developed their metadata, the next step is to publish that metadata in the DoD Federated Data Catalog. DoD Federated Data Catalog, which refers to the DoD Data Catalog and other Federated Data Catalogs. It is important to note that metadata and the cataloging of metadata is not a static process. Metadata will evolve. The business rules regarding when and how metadata is applied will be part of the next round of guidance.

New/emerging capabilities (applications, services, platforms, etc.) should start applying the minimum metadata plus additional mission or functional specific metadata as soon as is practical. Legacy capabilities will take time and should be scheduled on a priority basis of value to the enterprise/mission to apply minimum amount of metadata. Legacy capability owners should start a dialog with the appropriate CDO or appropriate Data Steward on when and how to apply metadata. The Data Producers (which includes the origination moment in the DoD (e.g., sensor captured raw data, government acquired first instance commercial data, newly derived alternate data) shall capture and record the minimum metadata necessary for any consumer beyond the producer to be able to use the data. Follow-on guidance is needed and addressed in section 4.1 as part of next steps. There are various metadata implementation approaches available from industry. It is out of scope to provide a breakdown of those approaches. These will be addressed in other documentation. Appendix D provides a snap shot of some information technology specification standards currently available that satisfy some or all metadata attributes.

4.1 Metadata Application Use Cases

The initial application of metadata (functional or mission specific metadata) is usually performed by the Originator organization of the data asset. Below are three use cases representing the three different initial metadata application scenarios across DoD; application immediately upon creation; application at the appropriate time after creation; and application upon the first instance a data asset is acquired by DoD.

4.1.A The first use case is application of functional or mission specific metadata immediately upon creation of the data asset. Figure 2 is a depiction of Use Case #1. This is the direct application of metadata the moment a data asset (i.e., a report, any binary data, etc.) is created.

Figure 2: Metadata plus any functional or mission-specific metadata applied to the data asset immediately, in this example, when the report (a type of data asset) is created in the All Source Analysis System (ASAS).

The second application use case, Figure 3, depicts the application of metadata plus any functional or mission-specific metadata at an appropriate instances after the data asset is created. Examples include airborne or satellite generated data assets. In this example the date and time of creation and location information is applied by the sensor while the remainder of the metadata is applied to the data asset at the ground node. The bandwidth of the link between the sensor and the ground station is limited, especially in contested and highly contested environments. Adding all the metadata before transmission to the ground would increase the amount of bandwidth needed to communicate each data asset resulting in fewer data assets being transferred in a timely fashion and thereby degrading mission performance.

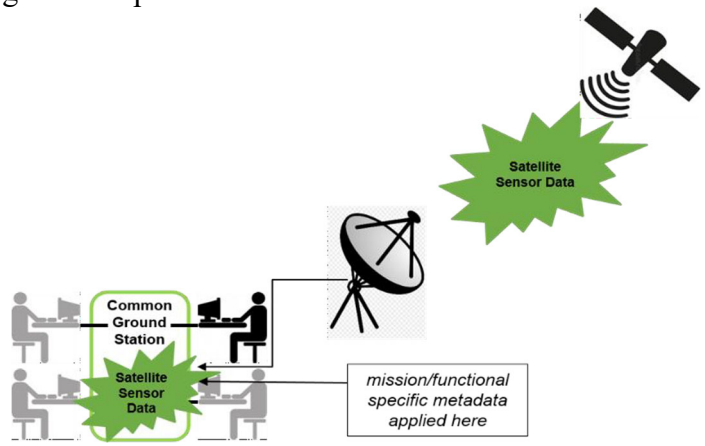

Figure 3: In this example the date and time of creation (a recommended field) and location (an optional field) are applied by the sensor while the remainder of the metadata is applied at the common ground station, which is the most appropriate time to apply those tags since the remaining metadata information (e.g., Authorization Reference) is not technically feasible to apply prior to transmission.

4.1.B The third application use case, Figure 4, depicts the application of metadata plus any functional or mission-specific metadata at the first instance a data asset that DoD acquires is introduced into the DoD IT environment. Examples of the application include the acquisition of commercial data assets or an adversary's hardware/data assets, or downloading publicly available data assets. This use case impacts the 'date and time of creation' metadata requirement. In this use case, the date and time created corresponds to the date and time the data asset enters the DoD IT environment rather than the date and time the data asset is actually created. It is important to note that the actual date and time information a third party data asset was created should not be lost in most cases.

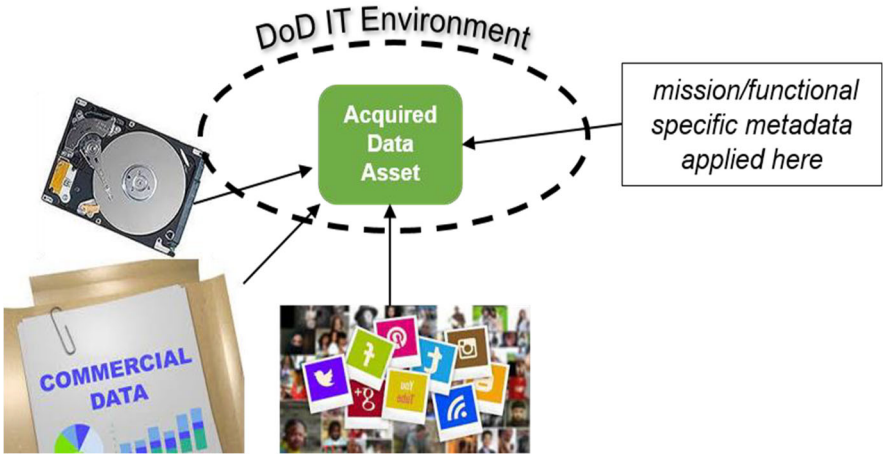

Figure 4: Functional or mission-specific metadata applied at the first instance the acquired data asset appears in the DoD IT Environment.

4.2 Metadata Fields

The metadata below describes the recommended fields to satisfy basic metadata inputs for Data Owners. These field names are provided to enable all data originators to map their specific equivalent term names to the enterprise provided values. Data originators should ensure the definitions are fundamentally equivalent. The list of suggested supplemental content is not exhaustive. In some cases, the supplement content maybe mandatory for a specific community or organization. An organization may always provide more content for a given metadata requirement, just not less. For example, an 'Originator' requires organizational details to satisfy the Originator data requirement. That same data asset may also provide location information or a specific office within the organization or a person's name.

Federal, DoD, and International policies will impact specific metadata information for specific activities. The IT technical specifications a capability developer chooses will also impact the metadata content and syntax (order and grammar). The general content requirements below do not supersede the content and syntax rules defined by a given policy or specification. The developer in coordination with the Data Steward and CoI SMEs must ensure they can satisfy the metadata content requirements with their technical approach. Beyond that, the developer should follow the policy and specification requirements. If the chosen technical solution does not satisfy mission requirements, the developer in coordination with the data steward and CoI SMEs should consider another approach to address the gap. The table below provides the recommended metadata content to satisfy the basic metadata attribute. It also provides supplemental (optional) content examples. The supplemental content examples are not exhaustive.

Metadata Label	Technical Description	Comments
Identifier	Identifier value	Unique ID within a local domain
Authorization Reference	A means of indicating a particular documented legal basis for mission activities associated with the creation, retention and use of a resource	
Originator	An entity (organization) primarily responsible for generating the resource. For DoD, "Originator" is synonymous with author, originator, and collector.	The Originator organization should not change throughout the data asset life cycle.
Custodian	ResponsibleEntity - This element and its children elements; Country, Organization, and SubOrganization; collectively represent the creating/originating organization that is responsible for the data object.	May perform mission and business data-related tasks such as collecting, tagging, and processing data, and may grant individual user's access to additional information beyond that of general systems, applications, and file permissions to perform such functions, where appropriate. The data custodian does not assume the legal or policy roles of the DoD Component. (IC Data Management Lexicon, 2020)
DataItemCreateDateTime	DataItemCreateDateTime element, which reflects the creation date of the data object.	
Description	Abstract	Human-readable
Format	Format Type	Machine-consumable
Security Classification	Classification Reference Document - Title & Date	
	Classifier - Originating Classification Authority; Organization Name; Organization Contact Information	• Author • Special Access Programs • Person's Name • Derivative Classification Authority with Organization Name & Contact Information. Classified By, Derived From, Declassify On, Person's Name is Optional and Downgrade On is optional • Retention Date • Recognized Community (a Combatant Command with a defined community, etc.); No Disclosure & Releasability • Person's Name; Person's Role; Purpose; Limited Uses; No Handling Restrictions
Disclosure & Releasability	Must have at least one of the three: *a Country/Countries, *Organization (e.g. NATO) *Category of People and/or Non-Person Entities	
Handling Restrictions	Handling Type to include Organization Name & Organization Contact Information	

4.3 Metadata Content Examples

Below are two metadata use cases. They illustrate how metadata is applicable standardized documentation. These examples also illustrate how an organization or CoI can include supplemental information to such documents.

The chart below reflects an example of Joint Chiefs of Staff approving a training event (Brave Squirrel 2025) and the mandatory metadata associated with the training report. As the report is disseminated amongst training participants and broader DoD the collective understanding throughout the community is enhanced by common metadata attributes.

Metadata	Recommended Content	Additional (Optional) Content Examples
Identifier	165313654A	
Authorization Reference	**Document title:** Exercise Brave Squirrel 2025 Order (EXORD) **Document Date:** 2024-02-05T01:01Z	**Organization Name:** Joint Chiefs of Staff **Organization Contact Information – Organization Mailing Address**: 1400 Defense Pentagon Washington, DC **Organization Email**: xxxx.xxxxx.xx.xxxxx@mail.mil **Organization Phone:** 703-555-5555 **POC Name:** Robert Sample officer, Maj Gen, USAF **POC Role:** Vice Director, Joint Staff
Originator	**Organization Name:** Joint Staff J7 **Organization Address:** JS Hampton Roads 116 Lakeview Pkwy, Suffolk, VA 23435 **Organization Phone:** 757-555-5555	**POC Name:** Theresa Sample event leader **POC Role:** Lead Event Architect, JS J7
Custodian	**Organization Name:** Joint Staff J7 **Organization Address:** JS Hampton Roads 116 Lakeview Pkwy, Suffolk, VA 23435 **Organization Email**: yyyy.yyyyyyy.yy.civ@mail.mil **Organization Phone**: 757-555-5555	
DataItemCreateDateTime	**Human Readable; Day;Month;Year;Time**:6/15/2025; 1500 UTC	
Description	**Abstract-** Results of training event Brave Squirrel 2025. The results include the successful and unsuccessful TTP and technical approaches applied as well as recommendations.	
Format	**Format Type:** Microsoft Word Document.	
Security Classification	**Classification Reference Document:** **Title:** Chairman's Instruction XYZ **Organization Name:** Joint Chiefs of Staff **Organization Address:** 1400 Defense Pentagon Washington, DC **Organization Email:** xxxx.xxxxx.xx.xxxxx@mail.mil	**Organization Phone:** 703-555-5555
Disclosure & Releasability	**Disclosure:** No disclosure restrictions **Releasability**: Open to the Public	
Handling Restrictions	**Handling Type**: None	

The chart below reflects the recommended metadata content necessary for a data asset developed in the following scenario. Diplomatic talks break down between the U.S. supporting Country P and Country M. Country M sends small teams of troops into Country P territory killing civilians and threatening U.S. interests. The U.S. decides to send in troops. U.S. Central Command crafts an operational plan and the order (the data asset) is issued. Operation Bully Pulpit is established with FVEY partners. The Combined Joint Task Force needs to share blue force track data.

Metadata	Mandatory Syntax	Optional Syntax
Identifier	1684136569G	SPC1234-F
Authorization Reference	**Document title:** U.S. Central Command Operational Order XYZ **Document Date:** 2023-03-05T01:01Z	**Organization Name:** U.S. Central Command **Organization Contact Information – Organization** **Mailing Address**: 7115 South Boundary Blvd, MacDill AFB, FL 33621-5101 **Organization Email**: xxxx.xxxxx.xx.xxxxx@mail.mil **Organization Phone:** 813-555-5555 **POC Name:** Joe Example officer, Gen, USMC
Originator	**Organization Name:** U.S. Central Command **Organization Address:** 7115 S. Boundary Blvd, MacDill AFB, FL 33621 **Organization Email:** yyyy.yyy.yy.civ@mail.mil **Organization Phone:** 813-555-5555	**Sub-Organization Name:** Combined Joint Task Force Bully Pulpit **POC Name:** Sgt Snuffy **POC Role:** Squad Leader
Custodian	**Organization Name:** Army Central Command (ARCENT)	
DataItemCreateDateTime	**Day;Month;Year;Time:** 2023-08-05T01:01Z	
Description	**Abstract-** Blue Force Tracking data for Operation Bully Pulpit	
Format	**Format Type:** eXtensible Mark Up Language	**Size:** 500 bytes
Security Classification	**Classification: Secret** (S) **Classification Reference Document: Title:** OpOrd XYZ **Organization Name:** U.S. Central Command **Organization Email:** xxxx.xxxxx.xx.xxxxx@mail.mil **Retention Date**: 2048-08-05	
Disclosure & Releasability	**Disclosure:** Category C **Releasability**: FVEY	
Handling Restrictions	**Handling Type**: None	

5 Future Considerations

a) Publish metadata technical patterns.
b) Share business processes and best practices for CoI and Data Stewards on defining their functional or mission-specific metadata.
c) Establish enterprise services that generate globally unique identifier(s) and enable enterprise sharing of mission-focused business rules.
d) Establish enterprise data services to support legacy system metadata interoperability.

Appendix A: Glossary

Term	Definition
Access Control	Granting or denying specific request for resources based on a defined set of criteria.
Audit	Recording the sequence of actions surrounding or leading up to a specific activity or event.
Chief Data Officer	A designated senior official responsible for the management of data as an asset and the establishment and enforcement of data-related strategies, policies, standards, processes, and governance. (IC Data Management Lexicon, 2020)
Community (also Community of Interest – CoI)	In relationship to data stewardship responsibilities, a group of people having an invested interest in the data sets and associated activities.
Correlation	Identifying relationships between entities within and across disparate data sets.
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. (IC Data Management Lexicon, 2020)
Data Access	The ability of a human or non-person entity to perform one or more operations on data, typically via service endpoints and Application Programming Interfaces. These operations may include the ability for data to be searched, retrieved, read, created, updated, deleted, manipulated, and executed. (IC Data Management Lexicon, 2020)
Data Asset	Any entity that is comprised of data. A data asset may be a system or application output file, database, document, or web page. A human, system, or application may create a data asset. (DoD 8320.02)
Data Lifecycle	A conceptualization of a birth-to-death 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. (IC Data Management Lexicon, 2020)

Data Lifecycle Management	Establishment and execution of policies and interconnected processes for managing data throughout the data lifecycle to support data management functions, such as data governance. (IC Data Management Lexicon, 2020)
Enterprise	The scope of an organization as defined by that organization based on a purpose or point of view. An enterprise may be a business, not-for- profit, government agency, or educational institution. An enterprise has a purpose, goals, and objectives. (refer to DAMA DMBoK: Data Management Body of Knowledge, 2nd Edition) For the purpose of this document, except when referencing the DoD Data Strategy or Mission Areas, enterprise refers to a DoD Component as identified: a. Office of the Secretary of Defense b. Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff c. Combatant Commands d. Office of the Inspector General of the Department of Defense e. Military Departments f. DoD Field Activities g. Other organizational entities, which includes the National Guard Bureau
Enterprise Data	Data that is used, shared, or generated with a particular point of view or perspective, generally DoD Component-wide, DoD-wide, or a functional area that involves many or all of the DoD Components. (Amplified from DAMA Dictionary, 2nd Edition)
Metadata	Information describing the characteristics of data; data or information about data; or descriptive information about an entity's data, data activities, systems, and holdings.
Protection	Processes, services, and methods used to accomplish the privacy, safety, confidentiality, integrity, availability and recovery of data. (IC Data Lexicon, January 2020)
Records Management	Activities involved with the creation, update, retention, and disposition of records.
Zero Trust	Method for protecting networks founded on the idea that no user can be trusted, and requires strong authentication methods for users, data, and devices.

Appendix B: Acronyms

Acronym	Definition
CDO	Chief Data Officer
CoI	Community of Interest
DAFAs	Defense Agencies DoD and Field Activities
DoD	Department of Defense
DoD Components	MILDEPs, OSD, DoD Agencies, CCMDs.
USC	United States Code

Appendix C: Key Terms

Resource Description:

a) Identifier - A universal, unambiguous (unique) local reference to the resource (modified from PO#3, NARA, and NATO).
b) Authorization Reference - The particular documented legal basis for mission activities associated with the creation, retention and use of a resource. (PO#3).
c) Originator– An entity (organization) primarily responsible for generating the resource. For DoD, Originator is synonymous with author, creator, producer and collector. (PO#3, NARA, and NATO).
d) Custodian - Organizational element that is legally responsible for making decisions related to the data asset (e.g. records management, declassification, eDiscovery, FOIA search.) (modified from NARA).
e) DataItemCreateDateTime – Date and time on which the data resource was created to include when a data resource came under government control (i.e. acquisition of third party data, etc.)
f) Description - A brief account of the resource. (PO#3, NARA, and NATO)
g) Format - Information about the file format, physical medium, or dimensions of the resource. (NATO)
h) Security Classification - A single indicator identifying the highest level of classification contained within a resource (NARA and NATO)
i) Disclosure & Releasability - Information pertaining to countries, organizations, or communities approved to receive the resource (PO#3, NARA, and NATO)
Handling Restrictions - Limitations not related to classification or releasability, such as Controlled Unclassified Information designations. (PO#3 and NARA)

Appendix D: References

Reference A: Deputy Secretary of Defense Memorandum: Creating Data Advantage

Reference B: DoD Data Strategy

Reference C: Program Management – Information Sharing Environment (PM-ISE) Priority Objective 3 (PO3), v1 – Data Tagging Functional Requirements, Dec 2014

Reference D: DoD Data Stewardship Memorandum and Guidebook

Reference E: National Archives and Records Administration (NARA) Code of Federal Regulations Subchapter B, chapter XII of Title 36, Code of Federal Regulations (36 CFR 1236.12) Title 44, United States Code

Reference F: NARA Bulletin 2015-04: Metadata Guidance

Reference G: Universal Electronic Records Management Requirements, Version 2 developed by the National Archives and Records Administration's (NARA) Requirements Working Group (RWG)

Reference H: NATO STANAGs (4778/5636/4774/5636)

Reference I: DoD Directive (DoDD) 8320.02 - Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense

Reference J: DODI 5200.48, “Controlled Unclassified Information (CUI)”

Reference K: DoD Directive 3115.18 DoD Access to and Use of Publicly Available Information (PAI), para. 1.2

Reference L: DoD Manual 5200.01 – DoD Information Security Program: Protection of Classified Information

Reference M: XML Data Encoding Specification for Intelligence Community Enterprise Data Header v 2019-Mar

Reference N: XML Data Encoding Specifications for Information Security Markings

Reference O: DoDI 5400.1, DoD Privacy and Civil Liberties Programs

Reference P: DoDI 5015.02, DoD Records Management Program

Appendix E: Mapping of U.S., NARA, and NATO Metadata

The below table provides a detailed mapping between the U.S. and NATO metadata and corresponding definition. The highlighted metadata elements identify the nominal metadata that should be included during time of creation, but must be before storage. The remaining metadata elements are applied throughout the life cycle of the data asset. As CoIs and organization's develop mission/functionally specific metadata they should refer to the full scope of the U.S. Federal Government and NATO metadata.

Federal Priority Objective #3	**U.S. Federal Gov Definition**	**Notes/Source**		**NATO Core Metadata**	**NATO Definition**	**Notes/ Source**
Green indicates selected for the minimum essential metadata						
				A Term with an '*' means this is a 'Group' containing mulitple metadata requirements		
Author	An entity primarily responsible for making the resource	DoD 5015.02-STD, Paragraph C2.T3.5		Originator	An entity primarily responsible for creating the resource, or the originator of the resource.	NATO Core Metadata
Contributor	An entity responsible for making contributions to the resource			Contributor	An entity responsible for making contributions to the content of the resource.	NATO Core Metadata
Description	A brief account of the resource	Record Descriptors (subject of title) - DoD 5015.02-STD, Paragraph C2.T3.2		Description*	Provides an overview of the contents of the resource - includes Description; Abstract; Table Of Content	NATO Core Metadata
Format	The encoding or data type of resource, providing information on how to interpret, open, or view the contents.	DoD 5015.02-STD, Paragraph C2.T3.9		Format*	Provides information about the file format, physical medium, or dimensions of the resource. Includes - Extent; Extent Qualifier; Media Format; Medium	NATO Core Metadata **This is not a one for one match**
Identifier	An unambiguous (unique) reference to the resource	RMA generated based on NARA assigned organizational identifiers. DoD 5015.02-STD, Paragraph C2.T3.1		Identifier*	An unambiguous reference to the resource within a given context. Includes - external Identifier and identifier	NATO Core Metadata
Language	The specific language in which the resource is written			Language	The language(s) of the content of the resource.	NATO Core Metadata
Authorization Reference	The particular documented legal basis for mission activities associated with the creation, retention, and use of a resource			Currently no corresponding NATO requirement		
Currently, no corresponding U.S. Requirement				Custodian	The organizational element that currently maintains the resource.	NATO Core Metadata
Publisher	The entity responsible for making a resource available ("releasing the resource")			Publisher	The entity responsible for making the resource officially available.	NATO Core Metadata
Spatial Coverage	The geographic region(s) about which the resource provides information			Coverage*	The temporal and spatial extent or scope of the content of the resource. Includes - Country Code; Geographic Encoding Scheme; Geographic Reference; Place Name; Region; and Time Period	NATO Core Metadata
Temporal Coverage	the time period(s) about which the resource provides information. This is separate from the date that the resource was created or published.					
Title	A name given to the resource			Title*	The official name of a resource. Includes - Title; alternative Title; and Subtitle	NATO Core Metadata
Topic Coverage	The subject(s) in the thematic / issue sense of the word (not the person the person sense) about which the resource provides information			Subject*	Provides information about the topic and the content of the resource. Includes - Subject; keyword; and Subject Category	NATO Core Metadata
				Type	The nature or genre of the resource.	NATO Core Metadata
Citation	A bibliographic reference			Currently no Corresponding NATO requirement		
Related Source	A link to another resource that contains complementary, contradictory, clarifying, or otherwise related information			Relation*	Provides information about references to related resource. Includes - Authorizes; Conforms to; Has Format; Has Part; Has Version; Is Authorized by; Is Defined by; Is Format of; Is Part of; Is Redaction of; Is Referenced by; Is Required by; Is Replaced by; Is Version of; Provides Definition of; Reason for Redaction; References; Replaces; and Requires	NATO Core Metadata
Confidence	A description of the level of belief in the accuracy of the information within the resource			Currently no Corresponding NATO requirement		

Event	Information pertaining to an event within the resource's lifecycle (e.g. authored, published, approved, rescinded, viewed, forwarded, etc.)	Record Dates - DoD 5015.02-STD, paragraphs C2.T3.3-4	Date*	Provides a calendar date and time associated with an event in the life cycle of the resource. Includes - Date Accepted; Date Acquired; Date Available; Date Closed; Date Copyrighted; Date Created; Date Cut Off; Date Declared; Date Disposition; Date Issued; Date Modified; Date Next Version Due; Date Submitted; and Date Valid	NATO Core Metadata
Lineage	Information pertaining to where a resource originated and where it has travelled or been routed		Provenance	A statement of any changes in ownership and custody of the resource since its creation that are significant for its authenticity, integrity and interpretation. The statement may include a description of any changes successive custodians made to the resource.	NATO Core Metadata
			Source	Reference to a resource from which the present resource is derived.	NATO Core Metadata
Maturity	Information pertaining to the resource's point within a lifecycle		Status	The current status of a resource.	NATO Core Metadata
			Version	The version of the resource	NATO Core Metadata
Currently no corresponding U.S. Requirement			Update Frequency	The interval (or frequency) of updates to the resource.	NATO Core Metadata
Retention Information	Information pertaining to the resource's authorized retention and disposition under the Federal Records Act		Records*	Information supporting record management tasks. Includes - Records Disposition; and Records Hold	NATO Core Metadata
Schedule Information	Information pertaining to the resource's assignment to and categorization under an authorized Record Schedule				

Federal Priority Objective #3	U.S. Federal Gov Definition	Notes/Source	NATO Core Metadata	NATO Definition	Notes/Source
Green indicates selected for the minimum essential metadata					
			A Term with an '*' means this is a 'Group' containing multiple metadata requirements		
Security/Entitlements Metadata					
Classification	a single indicator identifying the highest level of classification contained within a resource	DoD 5015.02-STD, paragraph C3.T1.1	Confidentiality	The confidentiality label assigned to the resource by the originator	NATO Core Metadata and STANAG 4774
			Metadata Confidentiality	The confidentiality label assigned to the metadata set associated with the resource	NATO Core Metadata
			Alternative Confidentiality	An additional alternative confidentiality label assigned to the resource	NATO Core Metadata
Currently no Corresponding U.S. Requirement			Policy Identifier	Provides the Governing Security Policy Authority which manages the security policy to which the confidentiality label relates and also provides an indication of the information domain that governed creation of the data item.	STANAG 4774
Disclosure / Releasability	Information pertaining to countries, organizations, or communities approved to receive the resource	DoD 5015.02-STD, Table C4.T.10	Context	Determines the dissemination of the information, beyond the set of NATO Nations. In combination with the Governing Security Policy, 'context' indicates the "Ownership." Information can be created in the context of co-operative activities, e.g. EAPC, in which the Governing Security Policy is applied.	STANAG 4774
			Releasable To	Used to expand the dissemination of information to additional entities outside of the context for which that information was created.	STANAG 4774

			Only	Used to restrict or limit the dissemination of information to specific entities and a sub-set of the entities within the context for which that information was created.	STANAG 4774
Handling Restrictions	limitations not related to classification or releasability, such as Controlled Unclassified Information designations.	Supplemental Marking List - DoD 5015.02-STD, Paragraph C2.T3.7	Currently no Corresponding NATO Requirement - portions of "Only" may apply		
Special Controls	Indicator(s) identifying the sensitive compartmented information, special access program/special access required, or related that are contained within aresource.		Additional Sensitivity	Used to indicate the sensitive nature of certain NATO information not conveyed by the Ownership or Classification; meaning that it is subject to additional stringent security regulations andprocedures.	STANAG 4774
Currently no Corresponding U.S. Requirement			Administrative	Used to indicate discretionary handling according to local, non- automated procedures or provide guidance about the disposition of information	STANAG 4774 this might correlate with the Handling Restrictions
Usage Rights	Restrictions on commercial, intellectual, or proprietary information, such as copyrights		Rights*	Provides information about rights held in and over a resource. Includes - Rights; Access Rights; Copyright; License; Rights Holder	NATO Core Metadata
Cells marked "Currently no corresponding requirement" does not mean there aren't communities both in the U.S. or NATO that need this metadata information. It means that the U.S. Federal Government or NATO have not indicated it is a broad requirement at this time.					

This table provides the detailed mapping of the U.S. Federal Government metadata requirements and the NATO metadata requirements. It has the metadata term, the corresponding definition.