DoD Manual 8180.01

Information Technology Planning for Electronic Records Management

Originating Component:	Office of the DoD Chief Information Officer
Effective:	August 4, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD 5015.02-STD, “Electronic Records Management Software Applications Design Criteria Standard,” April 25, 2007
Approved by:	John B. Sherman, Chief Information Officer of the Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02 and DoD Instruction (DoDI) 5015.02, this issuance implements policy, assigns responsibilities, and provides procedures specific to electronic records management (ERM) for DoD information technology (IT) acquisition, configuration, implementation, and maintenance of IT systems and services.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. IT systems and services, including locally implemented capabilities as well as those acquired or procured via:

(1) Federal Acquisition Requirement Compliant Defense Acquisition processes and procedures.

(2) DoDI 5000.02.

(3) National Institute of Standards and Technology in Special Publication 800-145.

c. Automated components of national security systems that create or store DoD or Federal records. For the purposes of this issuance, these components are considered IT systems.

d. Nothing in this issuance should infringe on Inspector General of the Department of Defense statutory independence and authority as articulated in the Appendix to Title 5, United States Code, also known and referred to in this issuance as "the Inspector General Act of 1978, as amended." In the event of any conflict between this issuance and the Office of Inspector General of the Department of Defense statutory independence and authority, the Inspector General Act of 1978, as amended, takes precedence.

1.2. POLICY.

a. In accordance with DoDI 5015.02, the acquisition, development, enhancement, and retirement of an IT system or service must incorporate records management (RM) curation and preservation considerations over the records' lifespans. These considerations include identifying and supporting the business and RM users that interact with the records as well as planning for IT capabilities and automation.

b. All records contained in the IT system or service must be managed in accordance with records schedules, which include disposition authorities approved by the National Archives and Records Administration (NARA).

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER.

The DoD Chief Information Officer oversees compliance with this issuance.

2.2. DOD COMPONENT HEADS.

The DoD Component heads:

a. Incorporate RM and preservation considerations for any IT system or service developed, acquired, or provided by the DoD Component, in accordance with this issuance.

b. Ensure that records contained in any IT system or service developed, acquired, or provided by the DoD Component are managed and scheduled in accordance with Subchapter B of Chapter XII of Title 36, Code of Federal Regulations (CFR).

c. Designate a records officer (RO) to administer the Component RM program.

d. Include the Component RO during planning of any IT system or service for Component internal use.

e. Include Component ROs of any customer Components during planning of any IT system or service to be provided to the customer Components.

SECTION 3: OVERVIEW

3.1. INTRODUCTION.

a. Overview.

All systems, services, and other IT supporting the DoD mission create, receive, or otherwise manage information and DoD records. To mitigate risk of loss or spoilage of DoD records and information, any acquisition, development, or upgrade of IT must consider RM pursuant to DoDI 5015.02. A discrete software tool or component cannot be the sole solution in the DoD IT environment; rather, an IT solution must consider how it will incorporate or integrate the building blocks of records and information management to achieve required RM capability in the DoD federated information enterprise. This approach provides a path for more automation and less burden to individual users to manage the records they create and access as they perform their assigned duties.

b. DoD Information Enterprise (IE).

All IT systems and services must operate in the DoD IE, which comprises both commercial and DoD capabilities, in accordance with DoDD 8000.01. The DoD IE levies security, interoperability, and other constraints on IT systems and services that may impact how ERM is supported. This issuance focuses on considerations and dependencies specific to RM that affect planning activities necessary for successful ERM within the DoD IE.

c. Alignment with DoD Data Strategy Guiding Principles.

This issuance's procedures support DoD's transformation to a data-centric organization that uses data at speed and scale. Specifically, this issuance documents what is necessary to design IT systems and services for compliance. Additionally, incorporating the procedures in the issuance:

(1) Supports the use of data, specifically valuable records stored as data, as a strategic asset.

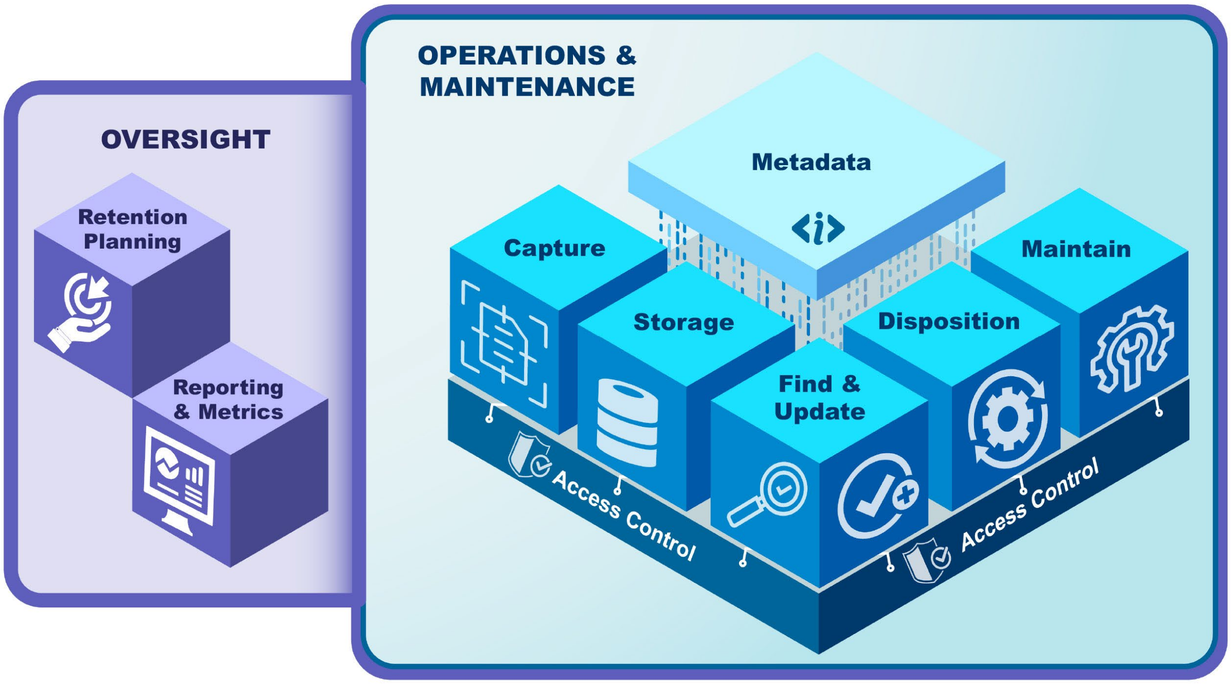
(2) Supports access and availability of the records for analytics and operational advantage.

3.2. ERM TECHNOLOGY PERSPECTIVE.

a. Building Blocks.

ERM has nine technology building blocks (see Figure 1). Each of these building blocks includes a set of considerations and requirements that are both unique to RM and historically have not been considered during the identification of requirements, system development or the acquisition stages of IT systems and services. Paragraphs 3.2.a.(1) - (9) offer a brief introduction for each building block, while Sections 4-12 provide more detail on their respective requirements.

Figure 1. DoD IE Building Blocks for RM



(1) Retention Planning.

(a) As a keystone of records and information curation, activities required in retention planning will result in identifying and understanding the information that will be created or managed in the IT system or service that can feed design decisions downstream.

(b) As a separate records management activity, DoD Component ROs work with NARA to appraise the information managed by the Component based on its archival value and value to the agency. Retention periods are defined and then scheduled with NARA as records schedule items. For example, military personnel records are of long-term value to the DoD and are scheduled as permanent, whereas temporary records are those of shorter-term value, ranging from months to decades. ROs routinely review and update records schedules as new datasets are created, or new uses of data are discovered.

(c) During retention planning for an IT system or service, information that is created or managed within the system is identified and the associated records schedule items are documented for use in further building blocks.

(2) Metadata.

(a) RM requires specific metadata that supports curation, automation, and governance focusing on information value, retention periods and holds, while leveraging metadata from other perspectives such as security for access control or context metadata for finding and retrieving.

(b) Automating ERM enables automatic metadata assignment whenever possible. To achieve this automation, metadata needs to be assigned when it is knowable. Upon creation of information, it is likely that an initial set of metadata will be known and can be harvested. It is expected that additional metadata can be added as information matures or metadata can be stored referentially. Metadata must be available when needed for all building blocks.

(3) Capture.

During records capture, information and associated metadata is saved into a digital format, whether unstructured as a file, part of a structured database, or a hybrid form. These information products are created or received and associated with metadata to identify that information and to support future use across its lifespan. Capture continues until:

(a) An information product is declared as a temporary or permanent record.

(b) All metadata is complete.

(c) The information product is placed under records control.

(4) Storage.

(a) Storage of data can be in-place in the creating or receiving system or service, a replacement system, a shared archive or RM repository, or a combination of these three options. Records include the associated metadata, records schedule items, and immutability status, which may be stored with the data or federated in linked data structures such as databases.

(b) Storage must be planned across the entire lifespan of the records that are managed in the IT systems or services. This applies to records whether stored within a government-owned or commercial service or cloud storage. If any permanent records are present, then storage needs to be planned for a minimum of 25 years with subsequent transfer to NARA.

(5) Find and Update.

Finding information requires that metadata and descriptive tags be available for searches in different contexts. Once found, the information product must be retrievable and exploitable throughout its lifespan for government business. Part 1220.32 of Subchapter B of Chapter XII of Title 36, CFR requires that records can be located (i.e., findable) through the duration of their lifespan. Once retrieved, records and information may be used in business processes resulting in new records or revisions if the record was not already finalized. In many cases, metadata may also need to be updated. This includes holds, which overrides a record's retention prohibiting further disposition.

(6) Disposition.

At the end of a record's active use, there are two options for disposition: destruction or transfer to NARA. To facilitate disposition, IT systems and services need to take into account ongoing monitoring of records retention periods to take disposal actions at the legally required time. Approximately 98 percent of all information products do not have permanent historical value and will be destroyed. Permanent records will be transferred to NARA.

(a) Destruction.

Once an information product has reached end of life and has been approved for destruction, it must be irrevocably destroyed. Temporary records may have:

1. Short lifespans and be destroyed within the lifecycle of the creating system;

2. Multi-decade lifespans, during which they are transferred to succeeding systems before they are destroyed; or

3. Any timeframe in between.

(b) Transfer to NARA.

Permanent records are transferred to NARA in accordance with the transfer date specified in a NARA-approved records schedule or when the records have been in existence for more than 30 years. NARA estimates that less than 2 percent of records are permanent and many IT systems or services may not manage any permanent records.

(7) Maintain.

To assure continued value to the DoD and in accordance with Part 1220.32 of Subchapter B of Chapter XII of Title 36, CFR, information products must be maintained as useable and trustworthy despite changes, refreshes, or updates to technology, policy, or strategies. This usability must be maintained through mundane changes to file formats, application software, operating systems, and storage media.

(8) Access Control.

Access to information is managed relative to mission or business roles, including proper authorization. For RM, access must be given to appropriate roles for managing records and information across each role's area of responsibility. This allows records managers to execute their duties efficiently.

(9) Reporting and Metrics.

The collection, analysis, and reporting of metrics to proper authorities supports governance and oversight. Records reports and metrics aid decision-making related to strategic direction, financial planning, and day-to-day operations.

b. Purpose-built Versus Utility IT.

Retention planning is fundamental to IT planning for RM. For any IT system or service, one of the two cases apply and will influence the planning for many of the building blocks:

(1) Purpose-built IT.

(a) Purpose-built IT systems and services are designed for a specific business or mission purpose and as a result, records created or managed within the IT system or service and their retentions can be identified during design time. In this case, the retention is either known or can be pre-defined based on the business or mission being automated by the IT system or service. Examples of purpose-built IT include business workflow, command and control systems, targeting systems, and the Defense Travel System.

(b) These solutions must have appropriate retentions included and managed as information products mature through the workflow or business process. For example, in a time recording system, approved time sheets must be retained for 3 years or until a Government Accountability Office audit. Once the record is 3 years old or is audited, it can be destroyed.

(2) Utility IT.

(a) Utility IT systems and services generate data that can be used for many business or mission purposes and have a variety of business or mission values. Examples of utility IT include general purpose word processing, chat, communications, spreadsheets, databases, office solutions, collaboration tools, and social media.

(b) Since the retention period is unknown at IT provisioning, a configuration plan to document default retentions for any data is needed and may be applied to workspaces, application types, or positions in the organization as best supported by the underlying IT. The plan will also include the set of retentions that may apply to that IT system or service during its operations.

3.3. STAKEHOLDERS.

a. Expertise.

Implementation of IT systems and services that meet the requirements of ERM and reduce risk to DoD records requires subject matter expertise in several areas. The traditional approach of pushing any records questions to traditional records staff cannot provide automated, scalable, and compliant solutions in the DoD IE.

(1) IT.

Implementation of ERM in IT systems and services that addresses the RM building blocks requires systems expertise. IT program participants must understand the technology requirements for supporting RM within the IT system or service. This includes:

(a) Communicating with records managers about the data and data stewardship within the system.

(b) Collaborating with records managers regarding retention requirements for the data.

(c) Applying the IT planning considerations discussed in this issuance to an IT program.

(2) Records Operations.

DoD Component records staff have detailed understanding of both the records that support the Components' mission and those that are products of that mission. Records staff provide input to many of the RM building blocks and are key partners in acquisition of any IT system or service. In the course of records operations, records staff maintain any IT project's associated records schedule and file plans. There are typically multiple personnel on the records staff with varying levels of responsibility. The DoD Component RO establishes and operates the Component's records program. Various records managers and records custodians have levels of responsibility in management of the Component records.

b. Groups.

There are four stakeholder groups that support successful RM in the DoD IE.

(1) IT Vendors.

Vendors are accountable for creating and maintaining functionality that supports DoD capability requirements with IT systems and services. For any IT vendor system or service that manages data for DoD, there may be varying degrees of native support for ERM and information governance. An understanding of this support is necessary when planning implementation of the vendor's product.

(2) IT Providers.

(a) IT providers develop, acquire, provide, and configure vendor capabilities and other services that operate within the DoD IE. The IT provider includes IT staff to create baselines and defaults for DoD-wide provisioning of the IT system or service for the customers. For the purposes of this issuance, IT providers may be internal to a customer organization or from a separate organization. In any case, the group that is responsible for the baseline activities is the IT provider.

(b) To effectively address RM considerations, the IT provider must have ERM expertise and access to those who understand records operations. In some cases, a single staff person may have both sets of expertise, but it is more often the case that different staff persons are needed to fill these roles. The staff will contribute to records related issues with customer IT planning, communications, training, and help desk.

(3) Customer Organizations.

Customer organizations articulate requirements for IT systems and services and validate the deployed configurations, including automation and artificial intelligence (AI) support.

(a) Financial staff may be involved to manage the IT budget.

(b) Business staff articulate requirements.

(c) Technical staff:

1. Must have a clear understanding of the IT systems and services supporting their enterprise and how they are integrated and interrelated.

2. Must provide data stewardship, coordinating appropriate constructs, information exchanges, and standardization to support the overall customer data landscape.

3. Collaborates with customer ROs and records staff for RM considerations.

(d) ROs and records staff:

1. Confirm that IT systems and services support RM operations.

2. Collaborate with customer technical staff and IT provider staff to support the IT systems or services through common RM terminology, training, and self-help support.

(4) End-Point Users.

End-point users may be restricted to read-only access but, for the purposes of RM, they are assumed to create data and information products in the course of their duties. Depending on the degree of automation of RM-related tasks, end-point users may need to know the value of their data and any associated record schedules or file plans. This is more likely to be the case when using utility IT. In the case of fully automated endpoint users, that understanding of the data and associated records value is built into the system or service.

3.4. USING THIS ISSUANCE.

a. Application of the RM Architecture Perspective.

Sections 4-12 describe each of the RM building blocks in more detail and provide both considerations and expected outcomes related to that building block. The RM building blocks provide an IT planning framework that minimizes risk to records during an IT system or service's acquisition.

(1) For each acquisition, the IT provider must consider the lifespans of the affected information products and determine whether the building blocks will be organic to the system or service or integrated with other systems and services in the DoD IE. For example:

(a) A timekeeping system is likely to maintain timesheets, draft timesheets, and reference data within a structured database. If the time and attendance have a retention of 3 years, then all the building blocks may apply as these records' lifespan is likely shorter than the life of the system.

(b) A word processing application is unlikely to manage the files created through its use. Aspects of the metadata and capture building blocks likely apply for electronic records created in the word processing system to automate tagging as much as possible. Integration is needed for storage and the rest of the building blocks to fully meet RM requirements.

(c) On the other hand, a messaging system might most efficiently manage most email records within the system because of the shorter expected lifespan associated with routine communications records. Aspects of storage, find, and disposition building blocks clearly apply in this situation and must be considered.

(2) Implementing facets of RM can challenge IT providers and their customers in the DoD IE. IT vendors, IT providers, customer in-house capability, and even end-point users all participate in creating and maintaining the solution and will have different perspectives to contribute to each of the building blocks while addressing the creation, use, lifespan, and final disposition of information products.

(a) Given the full spectrum of responsibility distribution and interdependence, there are no rules about which party has responsibility for each RM building block in any given IT system or service. Rather, the parties must collaborate to cover each building block. Further, each of the parties must clearly understand the boundaries and intersections of the functionality of their RM responsibilities with an eye toward the holistic RM capability across the organization's information environment.

(b) For example, in services architecture the original information product could be created by a desktop environment service; end up as a record in a destination purpose-built transportation or contracting system; be transferred to a component or shared services records archive such as Procurement Integrated Enterprise Environment's Electronic Document Archive; then destroyed or transferred to the National Archives.

(3) Customer ROs and the records staff are key partners for IT providers. They are accountable for the management of records within their Component, some of which are managed in IT systems or services. In many cases, there could be more than one customer for a particular IT system or service. Each customer records staff is the source of retention planning information and should work with IT provider and customer technical staff to ensure the retentions are properly applied and tracked in an ERM environment. These roles work together to optimize efficiency and automation that both minimize the manual burden on the end-point users and maximize the successful management of information and records, reducing risk to DoD records.

b. Using for Compliance.

To assess the compliance with the requirements for ERM, each of the nine architecture building blocks includes a set of desired outcomes for IT systems and services. The outcomes include compliance with NARA's Universal Electronic Records Management Requirements, as well as unique DoD requirements.

(1) RM Planning Artifacts.

Several of the outcomes required for compliance with this issuance are artifacts needed for IT planning. For example, this issuance calls for a data retention plan artifact that includes the enumeration of expected sets of data and associated retention requirements specified by records schedules. Any artifacts discussed in this issuance are described in detail in the appropriate building block section.

(2) RM Outcomes Checklist.

In Section 13, the outcomes from the building blocks are consolidated into a listing for use in assessing the readiness and coverage of RM functionality for an IT system or service. Each outcome provides a benefit to the planning process and needs to be reviewed by appropriate IT staff and records staff. In addition, application of the outcomes by multiple stakeholders for multiple purposes is included. For ROs, it may be a vehicle for communicating RM needs to vendors, IT providers, and customer organizations. For IT enterprise architects with the responsibility for RM, it ensures that RM considerations are addressed throughout the project lifecycle.

(3) RM Operations.

In Section 13, a list of RM operations explains the user tasks needed to support RM. If an IT system or service addresses the outcomes for each of the building blocks, then each operation will either be directly supported or part of a larger solution. This list is useful for testing and communication purposes.

SECTION 4: RETENTION PLANNING

4.1. OVERVIEW.

a. All records and information have a retention period based on the value of the information to the organization. The value includes business, mission, legal, and historical considerations. The information may be transitory (i.e., routine records of short-term value to the government); intermediary (i.e., those involved in creating a subsequent record); or of varying value requiring retention for anywhere from 6 months to the life of the republic as permanent records. ROs create and coordinate with functional managers an organization's retention strategy and maintain the retentions as a set of records schedule items within a records schedule.

b. Each records schedule item captures the rules for retention and disposition of the information and the approved disposition authority reference. All data and information managed in an IT system or service will have an assigned records schedule item that may be applied across the IT system or service, for a portion of the IT system or service, or to individual information products. Each subgroup of an organization will identify a file plan that includes a subset of the organization's records schedule for a specific use.

c. From an IT capability planning perspective, retention planning comprises identifying groups of data, associated records schedule items, their sources, accountable information owners, and responsible stewards for the data housed in each system or service. This information is necessary to develop processes and workflows to successfully manage the information across its lifespan. At the fundamental level, information product creators and end-point users, whether automated or human, must be able to link a record to a record schedule item when using the system or service. IT systems and services must be able to identify and take actions on information products based on its record schedule item.

d. Record lifespans will most likely not align with system or service lifecycle or their supporting contracts. During retention planning, IT providers and customer technical staff must plan for maintenance of records across consecutive systems or services. To support the full lifespan, IT providers and vendors are accountable for providing functionality for lossless data ingestion for immediate use and export of records.

4.2. REQUIRED INPUTS.

a. Mission or Business Process Information.

DoD IT systems and services create and manage information to support business and mission program managers by automating and enabling DoD business and mission processes. Identifying workspaces, analyzing business use cases, creating applications, and defining content types, user roles, or positions help uncover data that the IT system or service will create, receive, and manage as records.

b. File Plans and Records Schedules.

For any IT system or service, the IT provider must contact customer records staff for the associated records schedules or file plans that categorize any data in the system, identify records that will be managed in the system, and document the associated legal retentions.

(1) The customer ROs have incorporated administrative records schedule items from NARA's General Records Schedule (GRS), mission-specific retentions for their organization, and any special retentions of records in the IT affected by local, State, or foreign statutes (e.g., foreign nationals working on a DoD base).

(2) Existing digitized records schedules may exist in some form that can be reused.

(3) ROs and their records staff continually review and update retentions as new datasets are created or new uses of data are discovered. Retentions are approved by NARA through an appraisal process worked through the ROs.

c. Existing Data to Be Imported.

The capability to import and export long term records without losing content, context, or records status across multiple solutions may be required, particularly in cases when there is existing data to be imported into the IT system or service. Maintaining the integrity of the records lifespan requires the ability to exchange records retention and hold status across subsequent systems or services will need to be addressed in the planning process.

d. Policy.

DoDI 5015.02 establishes the policy for the DoD RM Program and includes applicable guidance for IT systems and services.

e. IT Vendor Assumptions.

To develop IT systems and services, IT vendors make assumptions in their architectures, feature sets, and user permissions. Understanding vendor assumptions regarding destruction, retention, and safe harbor will prevent inadvertent destruction of data that should be retained and inadvertent retention of information that should be destroyed. The IT provider ensures that RM outcomes are satisfied by the provided service, particularly when a third-party vendor technology is deployed.

f. Information about the DoD Strategic Plans.

The DoD seeks to improve information sharing and availability, assure security, identify efficiencies, and shorten IT deployment time. The DoD also seeks to leverage AI to analyze information value and use. Review of current DoD strategies during planning can provide guidance. Specific areas of interest are the DoD Records Strategy, DoD Data Strategy, and the DoD AI Strategy. These strategic focus areas may affect planning and management of records and information retention.

4.3. IT PROVIDER CONSIDERATIONS.

a. Determine if the IT System or Service is Purpose-built or Utility.

As described in Paragraph 3.2.b., the type of system impacts how data and records are most efficiently managed. Purpose-built systems, such as Defense Travel System or Defense Agencies Initiative, support common business processes, and the records and information created within the system has known value to the organization. Embedded IT capability, such as a command and control system or weapons platform, is purpose-built. Utility systems or services, such as office productivity systems, provide the ability to create content, but the business purpose or value of the content cannot be easily known.

b. Identify Possible Records Schedule Item Conflicts.

Any file plans and records schedules identified as an input to the planning process must be reviewed for potential retention conflicts. A conflict exists if two records schedule items appear to apply to the same data (i.e., it is not clear which records schedule item applies). Conflicts are more likely if there are multiple customer organizations using the IT system or service. Each organization's records may be governed by different records schedules. In this case, a means of electronically mapping the categories to specific customers may be required. Additional customer-required metadata, discussed in Paragraph 5.3., or some other mechanism could provide this electronic mapping.

c. Identify Data Groupings.

To plan retentions and make RM implementation decisions, the data that will be housed within the IT system or service must be identified. Documenting the data groupings can vary for each system or service depending on whether it is a purpose-built or utility IT system. Identifying data groupings should be considered carefully to make sure that all data has been identified and planned accordingly.

(1) Reference Data.

A common attribute of IT systems and services is to incorporate reference data for use in information processing. Reference data may be accessed through real-time connection to an authoritative source or may be copied and updated periodically from that source. The IT system or service does not have the authority to change reference data. Examples of reference data may range from a table of zip codes to weapons schematics to personnel lists. In the context of a specific IT system or service, reference data that has been copied into the system for convenience is non-record in accordance with Part 1222.14(b) of Subchapter B of Chapter XII of Title 36, CFR. IT providers can contact Customer records staff to confirm that the reference data grouping is non-record. Reference data is likely present in both purpose-built and utility IT systems and services.

(2) Records.

Typically, an IT system or service is in development or acquisition to fulfill a specific mission. It is likely that there will be records managed by the system that align to that mission.

It is easiest to identify these records in purpose-built IT systems and services as covered in Paragraph 3.2.b., since the business processes and their artifacts are well understood during planning and design. For utility IT systems, it can be more challenging. In some cases, it is possible that an entire organization's record schedule may apply to data in the IT system or service. For example, electronic messaging systems may generate content that is the record copy of a decision across any subject area for that account. In this case, it may make sense to identify data groupings according to the utility IT features or storage design components.

(3) Potential Records.

For some data groupings within the IT system or service, there may be potential records that are not yet known to be records.

(a) For automation purposes, it is important to understand that data groupings may be potential records because the data already has metadata known upon its creation that will be required once the potential record becomes a known record. In addition, these data groupings need to be understood to plan for retention and destruction.

(b) It is likely that any utility IT system or service has the most complex set of potential records. Time spent planning retention and workflow for these potential records allows for more automated support of end-point users. Customers will coordinate with IT providers to identify workflows, automation, and third-party RM integrations that will result in appropriately-scheduled records, overriding defaults.

(c) For data identified as potential records, the IT provider will default dispositions in accordance with Directive-Type Memorandum 22-001. IT providers are accountable for applying default disposition across the customers' configurations they support. Customers collaborate with IT providers to clarify where and how defaults will be overridden when a potential record is finalized as a record.

(d) Once the value of the information product becomes known through work processes or previous analysis, a records schedule item is applied and the content will be retained in accordance with that item. This record content may be moved from the original storage location and still be within the IT system or service, or it may be moved to another IT system or service. Copies of record content may remain in place under data management policies, and users should be trained or notified of the recorded content's location.

d. Consider When Transitory, Intermediary, or Position-based Retentions Apply.

Retention strategies enable ERM and deal with the scale of data sets being produced on a daily basis. These tools may be most useful when the IT system or service is a utility and when there are significant groups of potential records within the planned system.

(1) Transitory Records.

Transitory records (GRS 5.2 Item 010) do not document significant government business and may include messages coordinating appointments, transmittal documents that do not have substantive information, and task lists. Utility IT systems and services capability generates the bulk of these electronic records. The IT provider is accountable for implementing a retention and deletion strategy for applying to all transitory information in the DoD IE not otherwise covered by a customer records schedule item.

(2) Intermediary Records.

Intermediary records (GRS 5.2 Item 020) are often created during business or mission activities and reflect work in-progress. These records with emerging value can become finalized records or can be destroyed upon verification of the subsequent record's successful creation or when no longer needed for business use. Examples of records categories that might be considered intermediary records are working papers such as preliminary drafts, ad hoc reports, and meeting recordings that have been transcribed. Utility IT systems and services generate many intermediary records, which are likely associated with a specific business or mission function, and the final record emerges at the end of a transaction or decision workflow. The IT provider is accountable for implementing a retention and deletion strategy for applying intermediary status to all intermediary data in the DoD IE not otherwise covered by a customer records schedule items.

(3) Position-based Retentions.

IT systems and services may use position-based retentions, specifically email in accordance with GRS 6.1 "Email Managed under a Capstone Approach." This approach allows for the role of the account holder to be used to set the retention of each message in the account. This is particularly useful for efficient handling of senior officials' electronic files by managing all messages in senior officials' accounts as permanent records, thus eliminating the need to manage each message individually. Customer ROs are required to submit an associated NARA Form 1005 (NA-1005) to make use of position-based retentions for email. Use of position-based retentions can be considered but require submission of a schedule to NARA for approval.

(4) Applying Retention Strategies Based on Technology.

Records can be identified as transitory or intermediary based on the application type that created them or in groupings such as libraries, folders, or sites as long as this identification meets the criteria defined in GRS 5.2 IT providers map terms to avoid confusion. End-point users should not have to know vendor terms for the technical application types and structures that support them.

e. Develop the Data Retention Plan.

The data retention plan defines the set of data managed in the IT system or service and specific characteristics about the data needed to inform acquisition and development for RM purposes. Inputs ingested or received by the capability are identified as well as data created within the IT system or service. All the information is to be documented and assessed as part of the data retention plan. See Appendix 4A for data retention plan examples.

(1) Data Grouping.

Identify a grouping of data that will be managed within the IT system or service. In some cases, this may be a group that is aligned with a records schedule item. In other cases, it may align with the technology as discussed in Paragraph 4.3.d.(4).

(2) Type.

Document if this data grouping is reference data, records that can be identified, or potential records as described in Paragraph 4.3.c. The type of data grouping will affect the additional characteristics.

(3) Essential.

Identify if this data grouping is part of the customer's set of essential records for the organization's mission or purpose. These records are identified to establish a priority for protection and restoration in continuity of operations (COOP) planning pursuant to Paragraph 3.d. of DoDI 5015.02. Essential records require marking to indicate their status. This information is available from the senior official for the Component continuity program in accordance with DoDI 3020.42. Critical essential records may have non-digitized human readable renditions that must be tracked and managed as their digital counterparts.

(4) Sources.

Records can be created by the IT system or service during business or mission activity execution, imported or uploaded, bulk ingested, or referenced by linking to another system or service, such as a shared archive. When existing records are to be ingested into the solution for ongoing management, care must be taken to ensure that retention and hold status are included.

(5) Records Point of Contact (POC).

IT providers work with customer ROs and their records staff to identify the customer records POC accountable for managing any records that may be included in the data grouping. End-point users such as action officers, staff users, or automation can create and use organizational records, but they are not ultimately accountable for the proper management of records. Records ownership can be complex. Records are owned by the organization, the DoD, and the U.S. Government. The designated records POC for the owning DoD Component is the official authorized to approve RM functional activities such as disposal and application of holds.

(6) Records Schedule Item.

(a) Document records schedule item associated with that data grouping. This records schedule item provides the period of time for which the data must be available for use based on the value of the information to the organization. This information is available in the records schedules and file plans provided by the customer ROs. Utility systems and services likely create and house transitory and intermediary records, but storage strategies such as "manage in place" may require more full featured retention in a utility system. A permanent retention requires care during creation to ensure that trustworthiness is maintained through transfer to NARA.

(b) Ownership responsibility for these records will be retained by the originating organization for decades before the transfer process in Section 9. Any data groupings that do not have associated records schedule items identified may require customers to schedule that data. IT providers will work with customers to identify the appropriate records schedule item that indicates the pending status to protect this data from default deletion.

(7) Default Deletion Policy.

When the data grouping is a potential record or reference data, the grouping is non-record and there will not be a formal records schedule item applied via RM processes. In this case, a disposition is applied to enable automation and ongoing governance.

f. Plan for Rescheduling.

There will be events and changes to the mission that result in changes to the retentions identified in the original data retention plan. The IT provider will provide a capability for handling rescheduling of records to include bulk update of the affected records.

(1) Occasionally, NARA will determine that temporary records have historical value and the records must be rescheduled as permanent. Routine review of record value, including risk to the organization, may indicate that records must be retained longer or may be repurposed and will be rescheduled.

(2) In some cases, retention periods are shortened and the records managers advise whether the shortened period applies to records already in the data retention plan or only to those created in the future.

g. Unscheduled Records.

Many records and information are covered under the GRS or existing organization records schedules. Changes to mission or business processes or to the law may result in new categories of records that do not have an approved retention period. As the retention planning process works though approvals, these records must be clearly marked, not destroyed, and treated as permanent until NARA approves a retention. At that point, they are rescheduled. This can take several years, as the process includes a public review and approval of all destruction proposals.

h. Undeclared Records.

The intent of retention planning activities is to minimize the risk of having significant data groupings of undeclared records that have not been identified as records or potential records. End-point user or shared space should be examined to ensure that all records are identified. It is likely that undeclared records related to the IT system or service may be identified in the future.

i. Support Management of Records Schedules.

To realize RM, the data retention plan developed during planning needs to be loaded into the IT system or service, and changes managed over time. Ideally, the capability to manage the retentions will be automated, including loading of retentions, changing retentions, and applying schedule changes to affected records automatically. The IT provider is accountable for providing a means to update and digitize the records schedule.

4.4. OUTCOMES.

a. Table 1 enumerates a set of outcomes for IT systems and services to be used to assess implementation of retention planning requirements to support RM.

Table 1. Retention Planning Outcomes

ID	Requirement
01.01	DoD IT system or service is identified as either purpose-built or utility.
01.02	Any records schedule item conflicts are identified and resolved or addressed.
01.03	Data retention plan (completed in accordance with Paragraph 4.4.b.) defines the data managed by the IT system or service and the required characteristics of the data.
01.04	IT system or service manages multiple dispositions and retention periods assigned to a single record or a record set
01.05	IT system or service clearly marks and protects unscheduled records from destruction or spoilage until NARA approves disposition.
01.06	IT system or service provides the capability for authorized staff to define, load, and manage records schedules.
01.07	IT system or service automatically applies changes to records schedules to affected records and information.
01.08	IT system or service supports position-based retention if required in the data retention plan.
01.09	IT system or service supports GRS as defined in the data retention plan.
01.10	IT system or service creates or receives and manages digitized records schedule items for use within that IT system or service in accordance with existing DoD data and architecture standards.

b. Sample data retention plans are provided in Appendix 4A. Any data retention plan must include, at a minimum:

(1) Data grouping.

(2) Type (reference, records, potential records).

(3) Essential flag.

(4) Source.

(5) Records POC.

(6) Records schedule item.

(7) Default disposition policy, if applicable.

APPENDIX 4A: DATA RETENTION PLAN EXAMPLES

4A.1. OVERVIEW.

a. Retention planning is a key IT system and service planning activity that is specific to RM. In some cases, retention planning in general is done during any systems development project, but a focused effort on retention planning with knowledge of the presence of records, whether temporary or permanent, provides the foundation for compliant, efficient, and automated capability that can scale to the volumes of data generated in the DoD IE.

b. This appendix includes sample data retention plans. The examples used are notional IT system or services, with the information detailed in the data retention plan intended to be informative and illustrative of the concepts of this issuance.

c. The sample data retention plans are not published artifacts or official documentation.

4A.2. SAMPLE DATA RETENTION PLAN FOR A PURPOSE-BUILT IT SYSTEM.

a. Data Retention Plan.

A notional travel system is a purpose-built IT system handling DoD travel records for all DoD Components. Table 2 is a sample data retention plan for this system based on the concepts documented in this issuance.

b. Observations.

(1) Travel records are covered under GRS 1.1 Item 010, allowing the IT provider to provide management in place, including disposition for the life of the IT system or service.

(2) Travel records created in the last few years of the life of the system will be migrated based on coordination with customers.

(3) Travel records capture and retention labeling can be fully automated.

(4) Potential records and reference data do not have to be migrated by the IT provider at the IT system or service end of life and can be deleted as necessary in coordination with the customers.

(5) If technology management and information security records are managed within the system or service, they must be managed and migrated in accordance with their assigned records schedule items. If they are managed within the service, they are likely to be uploaded into the RM portion of the travel service, as RM is not the focus of the service and will not be used to create those types of records.

(6) This example does not include RM program records that will be generated upon disposition of records. The assumption is that those records are not managed in this service.

Table 2. Notional Travel System Data Retention Plan

Data Grouping	Type (Records, Potential Records, Reference)	Essential Flag	Source	Records POC	Records Schedule Item	Default Disposition Policy, If Applicable
Travel Records	Records	No	Created in Place	Customer Records POCs	GRS 1.1 Item 010	
Copies of Travel Records	Reference	No	Created in Place	Customer Records POCs	None	7-Year Deletion Policy: "Delete no more than 7 years from the date last modified"
Drafted Travel Data	Potential Records	No	Created in Place	Customer Records POCs	None	6-Month Deletion Policy: "Delete no more than 6 months from the date last modified"
General Technology Management Records	Records	No	Created in Place, Uploaded	Travel System Provider Records POCs	GRS 3.1	
Information Systems Security Records	Records	No	Created in Place, Uploaded	Travel System Provider Records POCs	GRS 3.2	
Information Access and Protection Records - Records tracking and controlling access to protected information	Records	No	Created in Place, Uploaded	Travel System Provider Records POCs	GRS 4.2 Item 030	
Information Access and Protection Records - Access control records	Records	No	Created in Place, Uploaded	Travel System Provider Records POCs	GRS 4.2 Item 031	

4A.3. SAMPLE DATA RETENTION PLAN FOR A UTILITY IT SERVICE.

a. Data Retention Plan.

A notional desktop productivity service is a utility IT service for use across the DoD as the desktop suite of tools. Within this service, it is likely that records with many different records schedule items will be created and managed. A key challenge is to plan for routine disposition of potential records and any additional automated processes for supporting RM. Table 3 is a sample data retention plan for this system based on the concepts documented in this issuance.

b. Observations.

(1) This type of system or service supports creation of records that can document any business process in the DoD. As well as encoding the GRS, many mission retention schedule items are necessary in coordination with customers.

(2) Capture of event plan metadata may be partially automated in conjunction with workflow definitions and storage container provisioning.

(3) Position-based retention, such as GRS 6.1 for communications type records such as email and chat messages, can be automatically provisioned and managed as coordinated with customers.

(4) Position-based capture of event plan metadata can be fully automated.

(5) Potential records and reference data do not have to be migrated by the IT provider at the IT system or service end of life and can be deleted as necessary in coordination with the customers.

(6) If technology management and information security records are managed within the IT system or service, they must be managed and migrated in accordance with their assigned records schedule items.

Table 3. Notional Desktop Productive Service Data Retention Plan

Data Grouping	Type (Records, Potential Records, Reference)	Essential Flag	Source	Records POCs	Records Schedule Item	Default Disposition Policy, If Applicable
Working Drafts	Potential Records	No	Created in Place, Uploaded	Customer Records POCs	None	7-Year Deletion Policy: "Delete no more than 7 years from the date last modified"
Chat Threads	Potential Records	No	Created or Received in Place	Customer Records POCs	None	6-Month Deletion Policy: "Delete no more than 6 months from the date last modified"
Senior Officials Email	Record	No	Created or Received in Place	Customer Records POCs	GRS 6.1 Item 010	
Administrative Staff Email	Record	No	Created or Received in Place	Customer Records POCs	GRS 6.1 Item 012	
All Other Staff Email	Record	No	Created or Received in Place	Customer Records POCs	GRS 6.1 Item 011	
Customer GRS Records	Records	Per GRS	Created in Place, Uploaded	Customer Records POCs	Per GRS	
Customer Mission Records	Records	Per RCS	Created in Place, Uploaded	Customer Records POCs	Per Customer Records Schedules	

Table 3. Notional Desktop Productive Service Data Retention Plan, Continued

Data Grouping	Type (Records, Potential Records, Reference)	Essential Flag	Source	Records POCs	Records Schedule Item	Default Disposition Policy, If Applicable
General Technology Management Records	Records	No	Created in Place, Uploaded	Desktop Service Provider Records POCs	GRS 3.1	
Information Systems Security Records	Records	No	Created in Place, Uploaded	Desktop Service Provider Records POCs	GRS 3.2	
RM Records - Tracking and Control Records	Records	No	Created in Place	Customer Records POCs	GRS 4.1 Item 010	
RM Records - Program Records	Records	No	Created in Place	Customer Records POCs	GRS 4.1 Item 020	
RM Records - Vital or essential records program records	Records	No	Created in Place, Uploaded	Customer Records POCs	GRS 4.1 Item 030	
RM Records - Copies of Vital Records	Records	No	Uploaded	Customer Records POCs	GRS 4.1 Item 031	
Information Access and Protection Records - Records tracking and controlling access to protected information	Records	No	Created in Place, Uploaded	Desktop Service Provider Records POCs	GRS 4.2 Item 030	
Information Access and Protection Records - Access control records	Records	No	Created in Place, Uploaded	Desktop Service Provider Records POCs	GRS 4.2 Item 031	

4A.4. SAMPLE DATA RETENTION PLAN FOR A PURPOSE-BUILT IT SYSTEM THAT INCLUDES OPERATIONAL RECORDS.

a. Data Retention Plan.

A notional command and control system is a purpose-built IT system that provides an integrated, near-real-time picture of the battlespace that is necessary to conduct joint and multinational operations. Table 4 is a sample data retention plan for this system based on the concepts documented in this issuance.

b. Observations.

(1) Command and control records are covered by individual DoD Component records schedule items.

(2) Command and control records capture and retention labeling can be fully automated.

(3) This IT system includes both temporary and permanent records.

(4) Some of the records created in this IT system are considered essential and require RM coordination with COOP and essential records reviews.

(5) Potential records and reference data do not have to be migrated by the IT provider at the IT system or service at end of life and can be deleted as necessary in coordination with the customers.

(6) If technology management and information security records are managed within the system or service, they must be managed and migrated in accordance with their assigned records schedule items. If they are managed within the service, they are likely to be uploaded into the RM portion of the command and control IT system, as RM is not the focus of the service and won't be used to create those types of records.

(7) This example does not include RM program records that will be generated upon disposition of records. The assumption is that those records are not managed in this service.

Table 4. Notional Command and Control System Data Retention Plan

Data Grouping	Type (Records, Potential Records, Reference)	Essential Flag	Source	Records POCs	Records Schedule Item	Default Disposition Policy, If Applicable
Targeting Information, Including Imagery	Potential Records	No	Created in Place	Customer Records POCs	None	7-Year Deletion Policy: "Delete no more than 7 years from the date last modified"
Operations Plan Information	Records	No	Created in Place	Customer Records POCs	Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, Vol. II 0500 Series	
Contingency Plan Information	Records	Yes	Created in Place	Customer Records POCs	CJCSM 5760.01A, Vol. II 0500 Series	
Deployment Plan Information	Records	No	Created in Place	Customer Records POCs	CJCSM 5760.01A, Vol. II 0500 Series	
General Technology Management Records	Records	No	Created in Place, Uploaded	Command and Control System Records POCs	GRS 3.1	
Information Systems Security Records	Records	No	Created in Place, Uploaded	Command and Control System Records POCs	GRS 3.2	
Information Access and Protection Records - Records tracking and controlling access to protected information	Records	No	Created in Place, Uploaded	Command and Control System Records POCs	GRS 4.2 Item 030	
Information Access and Protection Records - Access control records	Records	No	Created in Place, Uploaded	Command and Control System Records POCs	GRS 4.2 Item 031	

SECTION 5: METADATA

5.1. OVERVIEW.

a. Metadata is used across systems and services in a community of interest to assure authenticity and provide context for the records and, as such, is not specifically limited to RM. Customers are accountable for identifying customization of metadata necessary for automation of their business processes. IT providers are accountable for providing and configuring standard metadata sufficient to uniquely identify, capture, track, and dispose of records across the enterprise.

b. Upon creation, identification metadata are associated with data. As the data is designated as a record and matures throughout the business process and its lifespan, additional metadata is collected to provide business context, access controls, and retention status. IT providers identify opportunities to automatically capture metadata when it is knowable.

c. Metadata planning requires consideration of the RM use of metadata, including:

(1) Supporting metadata updates such as changes to records schedule items to facilitate reuse and repurposing.

(2) Logical linking among records.

(3) Reproduction or rendering records throughout retention.

(4) Migration of records across business uses, environments, systems, and services throughout the retention period.

d. Metadata elements may likely be for several purposes. For example, description metadata required by RM also supports finding and contextual use. As new uses for metadata are uncovered during the business and information use analysis, standard and previously identified metadata should be evaluated to determine if they are adequate to prevent duplication or overlap of metadata.

5.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. The data groupings included in Paragraph 4.4.b. guide the definition of any appropriate metadata beyond DoD mandatory metadata.

b. Metadata Standards.

Information about the definition and structure of metadata can be found in standards such as Intelligence Community Technical Specification “XML Data Encoding Specification for

Electronic Records Management," found in the DoD Information Technology Standards Registry (DISR), emerging standards, and community information exchange models. RM metadata provides lifespan state information and context. Application of metadata standards enables consistent, traceable, and understandable exchange of information across systems and services and maintain retention context throughout the records' lifespans.

c. Metadata Sources.

Sources of metadata across perspectives, business disciplines, information domains, and lifespan will provide insight about how to structure metadata and when to collect metadata input. For example, during creation in a utility system or service such as a word processor, unique identification information can be applied to the file, and a default business discipline might be "health care" if Defense Health Agency is the customer. Later, when the document is uploaded into a case file as draft justification for treatment approval, it can be assigned a records schedule item associated with health care case files.

5.3. IT PROVIDER CONSIDERATIONS.

a. Metadata Requirements.

Metadata requirements apply to purpose-built and utility IT systems and services. In the case of utility, there may be more business rules needed for metadata population of transitory and intermediary records as there are likely more potential contexts for those records. IT providers need to work with their customers to ensure metadata requirements by the business users and the records managers are understood.

b. Metadata Storage Mechanisms.

IT systems and services must provide a mechanism for storage of metadata. Technical structures such as database fields or tags to hold required metadata and metadata must be captured or updated as appropriate throughout the business process or record lifespan.

c. Categories of RM Metadata.

According to International Organization for Standardization (ISO) 15489-1:2016, six categories of metadata are required to properly manage electronic records. The categories are:

(1) Identity.

Information identifying the record.

(2) Description.

Information determining the nature of the record.

(3) Use.

Information facilitating immediate and longer-term record use.

(4) Event Plan.

Information used to manage the record, such as disposition information.

(5) Event History.

Information recording past events on the record and its metadata.

(6) Relation.

Information describing the relationship between the record and other records.

d. Required Metadata Elements for RM.

Required metadata for RM is listed in Table 5 and is based on NARA Universal ERM requirements; Information Community Technical Specification "XML Data Encoding Specification for Electronic Records Management"; the Office of the Program Manager, Information Sharing Environment's "Priority Objective 3: Data Tagging Functional Requirements Version 1.0", and DoD CIO Memorandum, "Federated Data Catalog - Minimum Metadata Requirements". Metadata element or tag identifiers named differently must be mapped to these names in documentation to support compliance evaluations.

(1) For each of the six categories of metadata required for RM, specific metadata elements are documented with a description.

(2) For some of the required metadata elements, population of the metadata with a value is mandatory, though it can vary on the timing of when it is mandatory. Some metadata elements are mandatory at the time of creation of the data, while others are mandatory at the time the record is complete. Section 6 discusses the records capture and its completion. Records cannot be complete until disposition instructions are populated, including the assignment of a records schedule item.

(3) Permission to edit metadata elements will depend on the role of the user and whether the record is complete. Edit permissions are discussed in Table 5 for each of the elements.

Table 5. Required Metadata Elements for RM

Required Metadata Element and Description	Timing of Mandatory Population, if applicable	Edit Permission
Identity Metadata		
File Name. The complete name of the computer file including its extension (if a content object is included).		No Restriction until Record Designation Date, then RM Role
Unique Identifier. An unambiguous (unique) reference to the resource. This identifier remains with the record throughout its entire lifespan. ("Identifier [Record ID]" as required for permanent records in accordance with NARA Bulletin 2015-04.)	Creation	Not Editable

Table 5. Required Metadata Elements for RM, Continued

Required Metadata Element and Description	Timing of Mandatory Population, if applicable	Edit Permission
Office of Record. Organizational element that is responsible for making decisions related to the data asset. ("Creator" as required for permanent records in accordance with NARA Bulletin 2015-04.)	Creation	No Restriction until Record Designation Date, then RM Role
Description Metadata		
Title. The name by which the record is formally known.		No Restriction until Record Designation Date, then RM Role
Description. A narrative description of the content of the record.		No Restriction until Record Designation Date, then RM Role
Essential Records Priority. Information indicating value as an essential record in accordance with Federal Continuity Directive 1.	Completion	RM Role
Spatial Coverage. The geographic extent or scope of the content of the record if record is related to locations.		No Restriction until Record Designation Date, then RM Role
Use Metadata		
Security Classification. Selection for the highest classification level of the record. ("Rights" component as required for permanent records in accordance with NARA Bulletin 2015-04.)	Creation	No Restriction until Record Designation Date, then RM Role
Access Control. Defines the roles and permissions for accessing data. Authorized staff who will be performing RM operations will need permissions beyond those provided to end-point users. Subject to guidance from DoD Cybersecurity Program.	Creation	Authorized Staff
CUI Indicator. Information about any types of CUI contained in the record in accordance with DoDI 5200.48.	Completion	Authorized Staff
Release Exemption. Information about any rights or restrictions held in and over the record, including access rights such as personally identifiable information or information retained in accordance with Sections 552 and 552a of Title 44, United States Code (respectively also known and referred to in this issuance as the "Freedom of Information Act (FOIA)" and "Privacy Act") in accordance with DoDD 5400.07 and DoDI 5400.11. ("Rights" component as required for permanent records in accordance with NARA Bulletin 2015-04.)		Authorized Staff
Usage Rights. Information about copyright and trademarks rights held in and over the record if		Authorized Staff

Table 5. Required Metadata Elements for RM, Continued

Required Metadata Element and Description	Timing of Mandatory Population, if applicable	Edit Permission
any. ("Rights" component as required for permanent records in accordance with NARA Bulletin 2015-04.)		
Rights Holder. A person or organization owning or managing intellectual property rights relating to the record. Applicable if usage rights are named.		Authorized Staff
Event Plan Metadata		
Record Designation Date. Date that the record is declared final (e.g., cutoff, publication, creation) and starts the retention period that will be used to calculate the disposition date based on the records schedule item. ("Date [Creation Date]" as required for permanent records in accordance with NARA Bulletin 2015-04.)	Completion	Not Updatable
Record Schedule Item. Identifier for the legal authority that empowers an agency to transfer permanent records to NARA or to carry out the disposal of temporary records. Typically found in a records schedule.	Completion	Authorized Staff
Disposition. An action taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure.		Authorized Staff
Hold Status. Used to indicate if a hold has been placed on the record, thus suspending disposition. Assigned and removed by RM users only.		Authorized Staff
Event History Metadata		
Past Event. Used to record changes to the records or metadata over the life of the record, if applicable.		No Restriction until Record Designation Date, then RM Role
Relation Metadata		
Has Part. A related record that is either physically or logically required to form a complete record.		Updatable by Using System
Is Part Of. A related record in which the described record is physically or logically included.		Updatable by Using System

(4) The unique identifier is a specific construct and not a default identifier as provided by a database row identifier. It should be assigned at data creation and stay with the information through destruction or transfer to NARA. This supports analysis and de-duplication of responsive records to electronic discovery for legal purposes and FOIA as well as identifying them as required by Part 1236.20(b)(1) of Subchapter B of Chapter XII of Title 36, CFR. It is up to the organization to define a strategy for unique numbering to prevent duplications or conflicts across the DoD. This should be considered in consultation with ROs.

(5) Managing holds on records requires the ability to capture and manage information about the hold itself as well as to apply the hold to responsive records. Responsive records may include transitory and intermediary records. The metadata structure should include these elements.

(6) Transitory records will be editable until they are destroyed. If customers choose to override this default with explicit retentions, they must define the record designation date and any trigger for its assignment.

(7) Intermediary records may not have a record designation date until a triggering event such as publication, transaction completion, or final signature. Until that point, these records are editable. Until the record designation date is assigned, business rules can be defined for setting Date Eligible, or records may be disposed based on the data retention plan.

e. Additional Metadata.

If not yet part of the planning for the IT system or service, consider additional metadata that may be needed for operations or compliance. While not specifically for RM, there may be other categories or elements of metadata to be identified.

(1) Nature of the Record.

Geographic records such as maps or photos of locations require location information. Files that require additional files to properly render require relational link information. Communities of interest may have defined standard metadata standards for contextualization and use in specific business disciplines such as those found in the National Information Exchange Model.

(2) Business Processes.

Additional metadata elements may be included in the metadata set as identified by RM staff and business users. Metadata elements may be added to support business and organization policy, processes, and procedures. Adding these elements includes understanding the potential lists of values as well as how the assignment of this metadata may be made automatically.

f. RM Metadata Plan Development.

The RM Metadata Plan identifies the specific metadata needed for performing RM operations. For executing disposition of data, the metadata is specific to RM. For identification and use of data, the metadata is defined through other data functions (e.g., access control), but required for successful and efficient RM. In some cases, metadata values may be ingested from authoritative sources.

(1) Metadata Element.

Identify and list each metadata element required for the IT system or service.

(2) RM Requirement.

Determine if the metadata element is required for RM.

(3) Timing of Mandatory Population.

Determine if the metadata element is required to be assigned a value at creation or completion. If there are additional business rules for populating metadata for the IT system or service, they can be noted here.

(4) Sources and Structures.

Consider potential sources for harvesting the metadata and also the structure for its storage. There is guidance and specifications that apply.

(a) Metadata elements are populated throughout the information lifecycle. Metadata can be extracted or inherited from business processes, workflows, and system environments. Elements can be set as organizational, process, or user defaults. Elements may be input by end-point users. As shown in Table 7, the source column identifies where the metadata value may be extracted.

(b) In order to exchange metadata, schemas are needed to set the overall structure of the metadata. In many cases, metadata schemas can set common components such as dates, names, and places, and there are metadata schemas specific to disciplines.

(c) ISO 23081-2:2009 should be referenced to work through conceptualizing and implementing metadata management schemas. A metadata management schema is required for new systems or services and should address responsibility for implementation.

1. Legacy systems or services should document the as-is schema during routine updates to verify that all mandatory metadata is being captured.

2. Vendors provide certain elements out of the box to allow their products to operate and to allow for some configuration by IT providers.

3. IT providers configure vendor products to meet customer needs.

4. IT providers configure automated harvesting of metadata and identify any metadata that will be needed from customer endpoint users.

(d) Changes to the systems or services or to the business processes for new functionality, improvements, and repairs may require adjustments to the metadata schema, sourcing, and method of population.

(5) List of Values.

Wherever possible, metadata options should be extracted or inherited, or constrained to a standard listing such as release exemptions. Customer organizations should be able to define defaults and picklists that can be updated by users with appropriate permissions.

(6) Default Value.

If applicable, identify an initial default value for the metadata element.

(7) Business Rules.

Document rules to be incorporated into the IT system or service to harvest or assign values to the metadata element based on business processes or rules.

5.4. OUTCOMES.

a. Table 6 lists a set of outcomes for IT systems and services to be used to assess implementation of "Metadata" building block requirements to support RM.

Table 6. Metadata Outcomes

ID	Outcome
02.01	Metadata structures and sources are identified based on the disposition and use of the data groupings in the data retention plan.
02.02	RM Metadata Plan is completed according to Table 7, defining the metadata requirements, sources, and additional characteristics.
02.03	Business rules for harvesting metadata are documented as part of the metadata plan. Purpose-built systems automatically assign metadata relevant to the supported business processes. Utility systems automatically assign metadata in accordance with organization's defaults and policies.
02.04	IT system or service includes unique identification metadata to support retention management, finding and updating, access control, reporting, and disposal.
02.05	IT system or service assigns default, inherited, or harvested metadata values with the ability for humans to overwrite when appropriate.
02.06	IT system or service incorporates metadata into or links metadata to the content or data.
02.07	IT system or service keeps metadata synchronized.
02.08	IT system or service exchanges metadata using a standard format registered in DISR.
02.09	Additional metadata to support business and organization policy, processes, and procedures is identified and documented in the RM metadata plan as appropriate.

b. Table 7 defines a planning artifact to specify the RM Metadata Plan for an IT system or service.

Table 7. RM Metadata Plan

Metadata Element	Required Flag	Mandatory Timing	Sources & Structures	List of Values	Default Value	Business Rules
Elements Required for RM						
File Name	X					
Unique Identifier	X	Creation				
Office of Record	X	Creation				
Title	X					
Description	X					

Table 7. RM Metadata Plan, Continued

Metadata Element	Required Flag	Mandatory Timing	Sources & Structures	List of Values	Default Value	Business Rules
Essential Records Priority	X	Completion				
Spatial Coverage	X					
Security Classification	X	Creation				
Access Control	X	Creation				
Release Exemption Indicator	X	Completion				
Usage Rights	X					
Rights Holder	X					
Record Designation Date	X	Completion				
Records Schedule Item	X	Completion				
Disposition	X					
Hold Status	X					
Past Event	X					
Has Part	X					
Is Part Of	X					
Other Elements for Mission, Architecture, or Legal Compliance						

SECTION 6: CAPTURE

6.1. OVERVIEW.

a. Records capture functionality is needed to place records and associated metadata under records control for disposition and access purposes. For certain activities this functionality may be built into systems so that the capture of records and associated metadata is simultaneous with creation of the records. For other activities, this functionality may require that the record be moved into a different system from its creation.

b. An underlying goal is to automate capture of any available metadata in the system, which reduces manual metadata capture by end-point users or administrators.

c. Capture is complete when the required metadata as discussed in Section 5 is assigned and associated with the record. A complete record contains not only the content, but also the metadata and contextual information necessary to document an official transaction or activity. A complete record meets the requirements to document evidence of organization, functions, policies, decisions, procedures, and essential transactions of DoD pursuant to Chapter 31 of Title 44, United States Code.

d. A complete record includes enough metadata to understand the organizational processes that produced the record and any linked records. The complete record provides for reliability, integrity, authenticity, accessibility, and security through-out their lifecycle.

e. DoD IT planning for acquisition and updates to IT systems and services includes consideration of all the aspects of capturing a record. The activities for capturing records may not happen in a specific sequence and, as discussed in Section 5, metadata information may come from many sources.

6.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. During planning for capture, the data groupings will be examined to determine when and how the data and associated metadata is captured.

b. RM Metadata Plan.

As described in Paragraphs 5.3.d.-e., required and additional metadata elements provide the framework for the needed operations in the capture phase to populate metadata. Planning for harvesting this metadata is discussed in Paragraph 6.3.

6.3. IT PROVIDER CONSIDERATIONS.

a. Workflow and IT Asset Determination.

IT providers work with customers to identify workflows and existing IT systems or services that can be exploited for records capture. Providers will work to automate the capture accordingly. In utility IT system and services, a capture workflow must be identified, otherwise the process defaults to end-point users and significantly complicates compliance.

b. Metadata Assignment.

Capture includes assigning the identification, descriptive, use, event plan, and relation metadata included in Table 7. Some of this metadata may have been assigned at creation or during the business process

c. Event Plan Metadata Assignment.

(1) During capture, records are assigned or linked to event plan metadata that define the retention for the record and provide references to records schedule items. Retention of a record can be based on different types of conditions translating to different types of disposition instructions as discussed in Paragraph 9.3.b.

(a) The calendar date such as the creation or modification date is often used to determine retention.

(b) A future event, such as military officer retirement or successful end of test may trigger retention.

(c) Mixed triggers involve events and time.

(2) When retention tracking is provided by a non-organic capability, application programming interfaces (APIs) or other interfaces allowing access to perform RM functions are required.

(3) Refer to the disposition instructions and contact the customer ROs for more details on disposition.

d. Finalized Record Becomes Immutable.

Once an explicitly applied retention period has begun, the recorded data may no longer be changed or deleted. It becomes immutable. Transitory or intermediary data does not become immutable unless it is subject to a legal or other hold. Changes to metadata of temporary records, permanent records, and records subject to hold are based on permissions and largely restricted to RM and other internal controls staff. Changing the length of an ongoing retention should not remove immutability of the recorded object.

e. Planning Records Capture for Data Sources.

Each of the sources for the data identified during retention planning should have planned capture functionality and activities.

(1) Record capture should be built into end-point users' daily work activities. Upon data creation, the data retention plan may allow for all targeted data to be placed under records schedules such as GRS 6.1 for email. Records created as products of workflow or transaction processing would be considered complete at the end of the process if all the associated metadata was collected and linked to the product.

(2) Information can be received from external sources. This includes one-at-a-time records and bulk uploads or transfers from other systems. One-at-a-time requests and submissions can arrive through email, web interface, or paper mail that is scanned or otherwise digitized.

(3) Records can be shared through interoperability. Each organization is responsible for properly assigning metadata and managing the stored copies of records from other organizations based on the value of that information to the organization.

(4) Projects to convert non-electronic records to electronic formats are specifically capture activities and will include validation support. These projects can include scanning or capturing information from forms into a structured format that will be used to recreate the record document (e.g., copying information from a legacy paper such as a DD Form 214, "Certificate of Uniformed Service," from which a new document is created upon request from the veteran or their family member(s)).

6.4. OUTCOMES.

Table 8 enumerates a set of outcomes for IT systems and services to be used to assess implementation of "Capture" building block requirements to support RM.

Table 8. Capture Outcomes

ID	Requirement
03.01	IT system or service clearly and visibly identifies finalized records.
03.02	IT system or service harvests and assigns metadata upon save, send, or receipt of data.
03.03	IT system or service assigns disposition or event plan metadata harvested from environment, via defaults, or from end-point user selecting pick list item.
03.04	IT system or service calculates and assigns the record designation date for temporary and permanent records.
03.05	IT system or service harvests and assigns the Office of Record or other entity accountable for disposal to all captured information.
03.06	IT system or service identifies essential records status.
03.07	IT system or service harvests and applies exemptions and exclusions for purposes of FOIA and Privacy Act compliance.
03.08	IT system or service provides an industry standard mechanism for accepting records from external automation.

Table 8. Capture Outcome, Continued

ID	Requirement
03.09	IT system or service automatically populates metadata to uploaded or ingested records and information.
03.10	IT system or service enforces immutability of temporary or permanent record content.

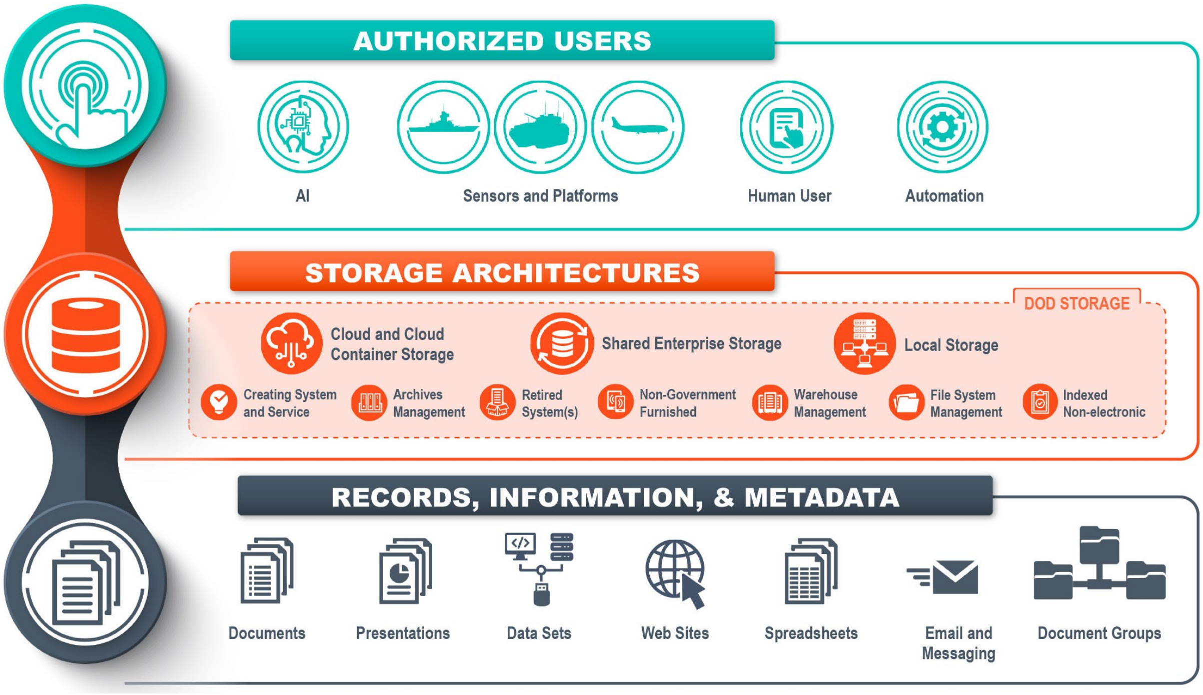
SECTION 7: STORAGE

7.1. OVERVIEW.

a. The data retention plan requires that a storage strategy must be planned and managed to cover the lifespan of the records in the DoD IE. This applies to records stored within a government-owned data center, commercial cloud storage, or hybrid strategies. If permanent records are present, then this requires planning and managing storage for at least 25 or more years with subsequent transfer to NARA.

b. Each IT system or service provides or coordinates managed records and information storage as constrained by the DoD IE. Storage can be distributed, federated, or monolithic and is expected to change as systems and services are both improved or replaced, and technology enhancements are leveraged. As shown in Figure 2, storage strategy must support all types of data and information formats and support access, administration, and updates by authorized users. Section 10 describes the effects of technology changes on record authenticity across the lifespan of the record in more detail.

Figure 2. Storage Context



7.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. A storage technical approach for each of the data groupings will need to be planned.

b. Metadata Plan for RM.

As described in Paragraph 5.3.d.-e., required and additional metadata elements will need to be stored and linked with records.

c. Customer Storage Capabilities.

To understand options for storing records through their entire lifespans, any options available to the customer for possible transfer and management of records need to be identified.

7.3. IT PROVIDER CONSIDERATIONS.

a. Storage for Utility IT.

If the IT system or service is utility rather than purpose-built, then the retention of the data is not known at design time and is documented as a set of possible records schedule items in the data retention plan. In this case, the design and maintenance of interfaces with storage will be affected and should be considered closely. IT systems or services such as repositories and federated storage solutions are likely to be utility.

b. Storage Plan.

Planning the technical approach for storage will determine the degree to which interfaces are necessary and their level of complexity, and will document assumptions and requirements.

(1) Management in Place.

Managing records "in place" can involve several strategies. The IT provider and customers must have clear expectations.

(a) IT systems or services that organically provide retention tracking and access management over records in their own repositories are a type of storage approach in which the records are managed in place. An IT system or service repository may be subdivided to support access and responsiveness. Records may be moved or copied from the original subdivision into a records repository within the IT system or service. When this is the case, data not contained in the records repository are convenience copies and are managed using the default retention strategies.

(b) IT systems or services that do not natively support RM typically use APIs to track retention, access control, and RM related updates, dispositions, and holds of the IT system or service data. In this case, an interface manages the records. Access control is a consideration when managing in place using a non-organic RM system or service.

(2) Movement to RM IT System or Service.

With this approach, the IT system or service uses APIs provided by an RM IT system or service to move the records and associated metadata into the RM repository. As described in

Paragraph 7.3.b.(1)(a), data not contained in the RM repository are managed using the default retention strategies.

(3) Shared Archive.

With this approach, the IT system or service and a separate RM system or service use a shared archive or data warehouse for storage of records. The shared archive or data warehouse provides APIs for accessing, updating, and controlling the records. Data copied from these shared archives are managed using default retention strategies.

(4) Hybrid.

A hybrid approach can be adopted that considers usage patterns and retention periods for records. Records with shorter lifespans or significant uses may be kept in the IT system or service, while lesser used or older records could be transferred to an archival or RM system's repository. When records are moved in mid-lifespan, the retention periods continue and do not restart. Any time a record is copied to a replacement RM repository, copies left behind are managed using default retention strategies.

c. Linking.

When developing the storage strategy, consider if there are any records created or received by the IT system or service that are composed of multiple parts or reference other records. Any identified links must be maintained regardless of whether each end of the link is stored together or in different files or data assets. It may be necessary to maintain referential indicators across data assets.

(1) Metadata.

As discussed in Section 5, metadata serves many different purposes: access control, retention management, identification, finding support, etc. These metadata sets can be distributed and federated or monolithic to the system or service housing the records. Links and references must be maintained throughout the records' lifespans to assure access, usability, and trustworthiness of associated metadata.

(2) Record Parts.

Some records require additional data to be contextually complete or fully useful. For example, font files can be referenced in PDF or the fonts can be embedded. To render properly, referenced font files should be included to support referencing. Other records can be part of a greater record such as an Adobe portfolio or attachment on an email. Where the record is not autonomous and requires additional files for use, links to the additional files are required for permanent records. The associated metadata elements must be considered in the storage plan.

(3) Other Records.

Records can reference other records, such as versions, renditions, references, or web links. Link information may be stored in metadata or embedded. Links should be referential and not named file paths as storage management frequently changes file paths. For additional guidance on link depth for storing web records see NARA Bulletin 2014-02.

d. Cloud.

Cloud and managed shared storage remove visibility to physical storage systems and locations and abstract the concept of storage boundaries as a limiting structure to user's functional access. As a result, APIs for accessing storage need to fully support RM functions such as irrevocable deletion, searching, retrieving, and updating metadata across multiple collections in an organization as well as managing holds.

e. Preservation of Permanent Electronic Records Beyond Decommissioning

NARA does not currently accept the transfer of permanent electronic records before the specified age in the records schedule item. If the IT system or IT service is archived or decommissioned before the time of accessioning of permanent electronic records and the records are not migrated to a succeeding IT system or IT service, care must be taken to preserve the permanent electronic records in a NARA-approved format. Failure to do so must be reported as an unauthorized disposition to NARA.

f. COOP.

In addition to RM functionality, backup and restoration are critical to COOP in the face of incident or disaster. In IT systems and services that contain DoD records, backing up data and ensuring backup data is accessible helps to prevent unauthorized disposition of electronic records. COOP storage management includes strategies for restoration of essential records in priority order of importance to the organization and its missions. Backup and restore strategies should also assure that legally destroyed records and information are not inadvertently restored in a COOP scenario. Some critical essential records may be identified for COOP storage in non-electronic format. These records are managed in parallel with the digital renditions.

7.4. OUTCOMES.

Table 9 enumerates a set of outcomes for IT systems and services to be used to assess implementation of "Storage" building block requirements to support RM.

Table 9. Storage Outcomes

ID	Requirement
04.01	Storage plan is defined to include the technical approach for records storage, metadata storage, and any needed linking across the lifespan of the records.
04.02	IT system or service maintains trustworthiness of the record and its associated metadata across storage architectures and strategies.
04.03	Storage architecture protects set of essential records needed for COOP.
04.04	IT system or service plans for storage of the record and its associated metadata for the required lifespan of the records as defined by their retentions.

SECTION 8: FIND AND UPDATE

8.1. OVERVIEW.

a. Finding data requires that content, metadata, and descriptive tags are visible for searches in different contexts. Different user roles require access to role-related metadata fields and configurations to find responsive records. For example, a business process user would be limited to searching for records related to the business process using identity and descriptive fields. An RM user would search on event plan fields and retention dates in order to execute RM operations such as auditing records schedule item assignments or executing disposal actions.

b. Once found, the record must be accessible and usable throughout its lifespan for government business, legal obligations, and possibly historical reference. Regulation requires that records can be located, thus findable, through the duration of their lifespan pursuant to Part 1236.10(d) of Subchapter B of Chapter XII of Title 36. CFR.

c. Potential and draft records may never be officially finalized; however, these records are subject to finding and updating, and are subject to holds. Identifying and descriptive metadata must be assigned, retention associated and tracked, and holds managed.

d. Finalized record content is immutable; however, the metadata to find and manage the records may be updated according to the organization's business and RM roles. For example, an RM staff member may search the descriptive and identity metadata fields for records to apply a hold, so the hold metadata for that set of records would be updated. Once the hold is released, the metadata would be updated again. A business user might have referenced a draft document on a permanent PDF record. If that intermediary record has since been deleted, the reference link would be removed.

8.2. REQUIRED INPUTS.

a. RM Metadata Plan.

As described in Paragraph 5.3.e., metadata sets identify the metadata that will be primarily used to support finding and will also provide some insight into metadata elements that will be subject to update for business and management reasons.

b. Access Control Plan.

As described in Section 11, user roles have been identified that are allowed to find or update information or specific metadata elements.

c. Storage Plan.

As described in Paragraph 7.3., a storage plan will identify various storage areas for the data. The IT provider must use this plan to assure that the user roles identified in the access control plan will be able to access the various storage areas.

8.3. IT PROVIDER CONSIDERATIONS.

a. Availability.

Content and descriptive metadata must be available to end users, authorized auditors, and internal controls users to support finding records associated with records schedules and other RM activities. Formats that cannot be indexed such as TIFF or those with limited document properties should have additional metadata to describe the content and type of the record.

b. Minimum Search.

At a minimum, customers should be able to create multi-field searches with inclusionary and exclusionary criteria to limit and focus result sets from the records and retention metadata. Customers should be able to:

(1) Request an order in initial result sets and reorder them after query response.

(2) Save searches and result sets to reuse and share.

(3) Create, save, and reuse searches that recall records due for activities such as cutoff, transfer, destruction, or hold management. These searches should support identifying records that are close to a retention action so that evaluations for bulk transfer to replacement IT systems, services, or archives can be conducted.

c. Updates.

(1) As records go through the business processes and managed lifecycle, metadata will be added or updated as appropriate to the activity. Metadata structures are not added in this context, but IT providers also have requirements for finding and updating the structures that hold the metadata attached to the records as part of system maintenance.

(2) At creation, identity information will be applied that can later be used to find the records. After the record becomes finalized, the record designation date should be populated to allow retention to be calculated and managed.

(3) Workflows and business processes may add descriptive or collection information about the supported processes or mission to the metadata. Information such as title or keywords may be updated as the record matures.

(4) IT providers are accountable for providing the capability for permissioned end-point users to find and update records via records schedule items and file plan management capabilities.

(5) IT providers will provide capability for finding and updating as well as finding the records schedule items. Customers ensure that timely changes to records schedule items are available to IT providers if the capability for self-service updates does not exist.

d. Disclosure.

Records and information are subject to legal discovery actions and responsiveness to requests filed in accordance with FOIA and the Privacy Act. Generally, these requests are limited to a subject area or an individual, so descriptive subject or topic and identifying metadata are the most likely search targets. Some records are exempt from public disclosure and others are excluded. The DoD includes mandatory metadata to indicate exemption or exclusion status of records.

e. Hold.

Records responsive to requests for information may be subject to holds, also known as “freezes”, during which the records cannot be destroyed. Holds may be placed for different reasons from legal holds to holds needed for disposition reviews. Holds functionality requires a mechanism for defining and linking to a hold object or construct.

(1) RM staff use the hold management metadata to create a hold and link it to the affected records.

(2) Holds objects include metadata that can be searched, revised, and when applicable, can be updated to release the hold.

(3) Holds information is transferred with the associated records to new systems or to NARA and are addressed further in Sections 9 and 10.

f. Storage.

Searching should encompass the entire data set including associated metadata regardless of storage distribution. Location of related non-electronic information should also be supported.

g. Encryption.

Information is commonly encrypted during transmission and at rest. Users of some applications can apply encryption or password protection to content that may become a record. Encryption strategies in the environment or available to end-point users cannot prevent authorized users from finding, viewing, and updating the records and information. See Section 10 for additional information.

8.4. OUTCOMES.

Table 10 enumerates a set of outcomes for IT systems and services to be used to assess implementation of “Find & Update” building block requirements to support RM.

Table 10. Find and Update Outcomes

ID	Requirement
05.01	IT system or service enables authorized users to search content and metadata of the records regardless of file type or encryption.
05.02	IT system or service provides the option for search results to be presented in the order of relevance to the search term.
05.03	IT system or service enables delegation or reassignment of a search request to trusted agents, including any data produced from that search to government-designated personnel for authorized business purposes.
05.04	IT system or service enables authorized users (including automation) to access and update record content.
05.05	IT system or service enables authorized users (including automation) to update or assign metadata to records, including retention codes, as they mature and are used.
05.06	IT system or service enables authorized users to change the Office of Record of the information.
05.07	RM users can designate records be placed in a “hold” status and destruction ceased regardless of assigned retention.
05.08	RM users can release the “hold” designation of a record.
05.09	RM users can save and share searches.

SECTION 9: DISPOSITION

9.1. OVERVIEW.

a. There are two disposition options at the end of a record's active use: destruction or transfer to NARA. Approximately 98 percent of all records do not have permanent historical value and will be destroyed. Permanent records will be transferred to NARA.

b. Temporary records may have operational, mission or historical use to DoD for a duration of days to a long-term retention of decades. In the case of long-term retentions, it is often the case that the lifespan of the record will exceed that of the IT system or service in which it was created as discussed in Paragraph 10.1.c.

c. Disposition instructions may be triggered by a point in time, a specified event, or a combination of both. Disposition instructions may also include a retention period that must pass prior to the destruction or transfer.

d. Once data has reached end of life and has been approved for destruction, it must be irrevocably destroyed.

e. Disposition reviews can range in formality from pre-approval for automatic disposition to sign off on individual records by the accountable authority. Automation, including AI, can be useful in preparing material for disposition reviews by selecting and grouping data in review packages. Customers identify the records and processes that require disposition review. IT providers ensure default disposition reviews of records marked as essential to ensure that critical information is not lost.

f. Permanent records are transferred to NARA at the end of their authorized disposition as documented in the assigned record schedule item. Most permanent records have multi-decade lifespans with the DoD before being transferred to NARA. As a result, most will be transferred to succeeding systems, archives, or records repositories before their ownership is transferred to NARA. Records transferred to NARA will almost always require a disposition review.

9.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. The records schedule items and their retentions will guide planning for disposition.

b. Storage Plan.

As described in Paragraph 7.3., a storage plan includes the technical approach for records storage, metadata storage, and any needed linking across the lifespan of the records. This plan includes the existence and use of shared archives, records repositories, or data warehouses and provides information about standard or accepted formats.

c. Guidance for Transfer of Permanent Records.

Records staff can be consulted to identify the current guidance for transferring permanent records to NARA. Such guidance will include formats, metadata sets, submission document and processes for moving ownership of records from DoD to NARA. For any IT system or service that manages permanent records, this guidance is critical.

9.3. IT PROVIDER CONSIDERATIONS.

a. Implementation of Disposition.

All DoD IT systems and services will identify and implement routine automated and documented destruction.

b. Types of Disposition Instructions.

There are three types of disposition instructions codified in records schedule items. The type of disposition can affect the degree of automation and if a manual or external trigger might be required. In some cases, a disposition instruction may include more than one of the types.

(1) Time Disposition.

A disposition instruction that begins the fixed retention period at a specific point in time, e.g., the end of the fiscal year, can be automated most easily and requires only access to the system clock.

(2) Event Disposition.

A disposition instruction that specifies transfer or destruction to occurs when a specific event occurs can require more planning to be automated. How does the IT system or service receive the input that the event has occurred? Is a manual step required? Is a trigger received from an external automated process?

(3) Event-Time Disposition.

In some cases, the disposition instruction may include an event followed by a fixed time period prior to disposition. This type of disposition requires the same consideration as an event disposition. The time period after the event must also be accounted for during planning.

c. Unscheduled Records.

As described in Paragraph 4.3.e., there may be unscheduled records identified due to changes in business or mission. Such records must be treated as permanent until NARA approves an appropriate records schedule item. Unscheduled records are known to have value, but the retention has not been approved. Unscheduled records generally arise out of new programs.

d. Transfer to NARA.

Permanent records are identified at capture, and metadata necessary to document record history is captured throughout the records' active life.

(1) At the end of the retention period, permanent records are submitted to NARA in accepted formats with required metadata and documentation. Submitted records are retained until verification is received that they have been successfully ingested into NARA systems.

(2) Customer ROs are accountable for transferring permanent records to NARA. IT providers support customers by ensuring that qualified records in IT systems and services are transferred to NARA's Electronic Records Archive (or replacement) upon qualification or transferred to the customer designated location for ongoing retention. Customers must validate the transfer to make sure there is no loss of record content, metadata, or state. IT providers coordinate with customer RM staff to coordinate the transfer processes, protocols, and required documentation.

(3) Reports and metrics documenting the transfer processes are created, submitted, and managed according to the organization's record schedule.

(4) If permanent records scheduled for transfer to NARA are currently subject to hold, these records may be transferred but must include the details of the hold.

e. Destruction.

All transitory, intermediary, and temporary records are destroyed in a manner that is irrevocable. IT providers must provide a capability for destruction. Customers validate the destruction.

(1) Transitory Records.

DoD-wide defaults for potential records identified during retention planning allow for automated, non-reviewed disposal. The disposal process removes access to the records, holds them for the safe harbor period for recovery, then finalizes irrevocable destruction.

(2) Intermediary Records.

Many end-point users may want to keep draft records longer than a year for reference purposes if related projects are expected. This does not meet the definition of reference material and these files are still subject to electronic discovery for legal purposes and may present risk to the organization. As identified in the data retention plan, appropriate policies based on last modified dates should allow retention of commonly reused material while allowing automatic destruction of potential records, without disposition reviews.

(3) Temporary Records.

Destruction of temporary records may require disposition review and approval by the records managers who coordinate with the records owners. For example, a set of contract files that were closed 6 years and 3 months ago are now available for destruction according to the GRS. The system or service should notify the records manager, who reviews the records for the possibility of holds and notifies the customers. Upon approval by the records manager, the files can be destroyed. Customers may require some level of disposition reviews for some records categories, while others can be disposed of automatically.

f. Records Holds.

Records managers or other authorized personnel manage holds as discussed in Section 8. Records that are subject to hold may not be destroyed until the hold is lifted. Destruction for records that are eligible upon lifting of a hold may be immediately queued for review, approval, and destruction. Transitory and intermediary records subject to holds will be irrevocably destroyed upon release of the hold if the safe harbor period for original destruction has expired.

9.4. OUTCOMES.

Table 11 enumerates a set of outcomes for IT systems and services to be used to assess implementation of disposition requirements to support RM.

Table 11. Disposition Outcomes

ID	Requirement
06.01	IT system or service identifies records that are eligible for destruction.
06.02	IT system or service uses an automated or workflow process to destroy those records eligible for destruction.
06.03	IT system or service completes destruction of electronic records in a manner that protects any sensitive, proprietary, or national security information.
06.04	IT system or service retains a copy of all permanent electronic records transferred to NARA until receiving official notification that NARA has accepted legal custody of the records.
06.05	IT system or service removes or disables passwords or other forms of file-level encryption that prevent access to records before transfer to NARA.
06.06	IT system or service transfers permanent records to NARA in the preferred and acceptable formats in accordance with NARA Bulletin 2015-04.

SECTION 10: MAINTAIN

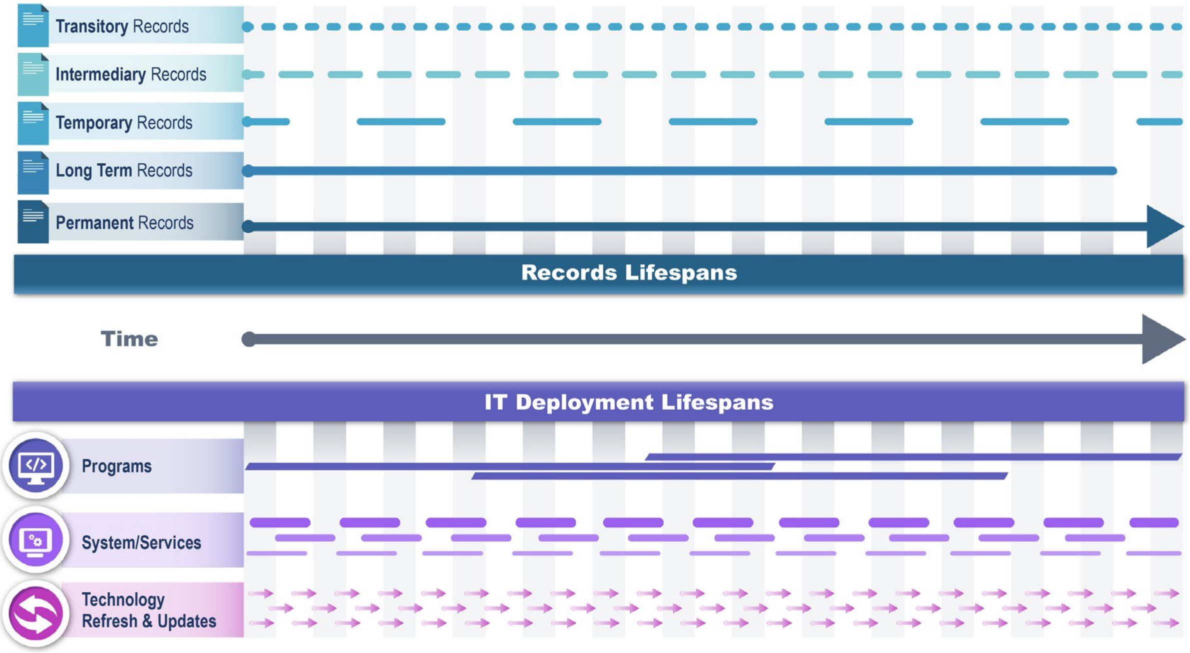
10.1. OVERVIEW.

a. To assure continued value to the DoD and to comply with statute, records must be maintained as findable, human readable, and trustworthy despite changes, refreshes, or updates to technology, policy, or strategies.

b. An IT environment continually changes with installation of fixes and patches, improvements, change requests, technology refreshes, updates to system or service requirements, acquisition changes to programs, and changes to standards and best practices. Security levies requirements for protecting information that includes digital signatures and encryption. Records are created in many formats by many kinds of software systems and applications, such as simple desktop applications, photo and video editing programs, complex robotics, or AI analytics. Despite all of these continual changes and the variety of record sources and formats, records must be maintained as trustworthy, accessible, and useable throughout their entire lifespans.

c. As shown in Figure 3, the lifespan of permanent records and temporary records with long term retentions are likely to outlive the lifecycle of the IT system or service in which they are maintained.

Figure 3. Lifespan of Records and IT Systems and Services



d. Temporary records may have lifespans from a few months to several decades and must be available to the DoD throughout their lifespan. Temporary records that outlive an IT system or service lifespan will be transferred to succeeding systems, archives, or records repositories before destruction and without loss or content, metadata, or state. IT providers are accountable for ensuring ongoing exploitability of housed records, including lossless non-destructive format translations and conversions. Customers validate translations and conversions. As with any set of records, customers may require some level of disposition reviews for some records categories, while others can be disposed of automatically.

e. Requirements to maintain access to records throughout their lifespan applies to records whether stored within a government-owned service or cloud storage.

10.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. The records schedule items and their retentions will guide planning for the Maintain building block.

b. Storage Plan.

As described in Paragraph 7.3., a storage plan includes the technical approach for records storage, metadata storage, and any needed linking across the lifespan of the records. This plan includes the existence and use of shared archives, records repositories, and data warehouses and provides information about standard or accepted formats.

c. Customer Storage Capabilities.

To understand options for maintaining records through their entire lifespans, any options available to the customer for possible transfer and management of records needs to be identified.

10.3. IT PROVIDER CONSIDERATIONS.

a. Purpose-built or Utility.

Purpose-built systems are more likely to house long term and permanent records and would require plans for moving those records into replacement systems or archival structures. Utility systems may also have long term and permanent records, though likely fewer than purpose-built systems.

b. Review the Data Retention Plan.

Revisit the data retention plan from the perspective of requirements to maintain records for their full lifespan. The plan specifies the records schedule items needed for the IT system or service and includes the possible record lifespans. As shown in Figure 3, records' lifespans, particularly long term and permanent records, are not likely to line up with IT lifecycles, so storage of records throughout the record lifespan must be considered. If the IT system or service include records with shorter-term lifespans, the ability to leverage automation of disposition of those records will reduce redundant, obsolete, and trivial information within the system as well as burden on end-point users and IT resources.

c. Maintenance Planning for Formats.

IT providers must plan for maintenance related to formats. IT providers need to:

(1) Identify formats used in the system or service by capabilities that create files to plan what may need to be transformed if it has a longer lifespan.

(2) Gather policy, best practices, or guidance for transforming, translating, and reformatting information, including acceptable error and loss rates.

(3) ISO 14721:2012 provides information about open archival information systems and includes discussions of how information archival changes over time.

d. Encryption.

Security requires that information be encrypted at rest and during transmission, which is usually handled by the storage and network capabilities. However, organizations may choose to add additional encryption requirements that they control. For example, a requirement might be included that requires email users to use personal keys to encrypt and digitally sign certain email messages. Unless these messages are decrypted before they are captured, they may trigger an unauthorized destruction for the organization because they cannot be accessed by operational controls for audits or responding to legal requests for information. The IT provider must ensure that encryption does not become a barrier for record availability.

e. Technology Refresh and Updates.

Technology refreshes include patches and fixes to software as well as updates to computing hardware and network devices. Virtual machines are software driven and changes to methods for managing virtual computers and networking devices are considered refreshes. Changes to strategy such as moving to a virtual environment or using software defined networks may impact access to records. Change management processes can provide information about what records may be impacted by changes to formats or other structure. Care must be taken to ensure records are preserved in the IT systems or IT services to the time of the legal disposition authority in the event of loss of vendor service, termination of the service, obsolescence of the IT system or IT service technology.

f. IT System or Service Change.

DoD acquisitions are limited by contract length and are routinely re-competed. These changes of contracted engineering or IT providers may change the supported system or service. While the name of the capability may stay the same, the contract may make changes that require updates to the system or service, and this can affect records. Additionally, changes to contracts bring change to responsibilities for holding and managing DoD records and information. Identification of follow-on IT systems and services may include updated or changed formats. Where feasible, save any temporary records, especially those with a long-term retention time, into a NARA preferred or acceptable file format in order to support future business needs such as

g. Program Change.

Programs generally have a defined life span and must be re-chartered or be replaced by a newly chartered program. This does not automatically change the IT system or service provided to DoD, but it does change program stewardship of the records and information. These changes may affect records such as a change in records ownership.

10.4. OUTCOMES.

Table 12 enumerates a set of outcomes for IT systems and services to be used to assess implementation of the Maintain building block to support RM.

Table 12. Maintain Outcomes

ID	Requirement
07.01	IT system or service maintains records in findable and readable formats regardless of the life of the system.
07.02	IT system or service supports publishing information in a digital format using a web-based interface for public facing systems and services.
07.03	IT system or service ensures that records and associated metadata are not encrypted in a manner that obstructs access by operational controls for audits or responding to legal requests for information.
07.04	IT system or service imports records and associated metadata maintaining relationships and record retention status.
07.05	IT system or service exports records and associated metadata maintaining relationships and record retention status.
07.06	IT system or service provides artifacts for imports and exports to be validated.

SECTION 11: ACCESS CONTROL

11.1. OVERVIEW.

a. Access to information is managed relative to mission or business role, including proper authorization, a valid need-to-know, and non-disclosure agreement. For RM, appropriate roles must have access for managing records and data across each role's area of responsibility. This allows records managers to execute their duties efficiently. Access levels change as the record status changes.

b. IT providers must collaborate with vendors to define access policy and roles to support RM functions such as tracking retention, updating retention, rescheduling, applying retention holds, and disposition. Customers integrate access policy and roles into their business processes and assign those who will fulfill required roles.

11.2. REQUIRED INPUTS.

a. Data Retention Plan.

As described in Paragraph 4.3.c., data groupings are identified and described during retention planning. This plan will provide information to inform the definition of roles and access requirements.

b. Access Restrictions.

IT systems or services and other components in the DoD IE may impose access restrictions on users. In the DoD, access to some IT assets requires training and certification for the different levels of access authorizations.

c. Vendor Access and Deployment Assumptions.

Any technology or component from a vendor that is used to deliver the IT system or service will include assumptions about how their capability will be configured and deployed. These engineering assumptions will affect how capabilities are bundled and what access is required to use them. In some cases, the IT provider may be required to staff authorized personnel to support multiple customers to reduce the number of people with administrative access to information their organization does not own.

d. Required RM Operations.

See Section 13 for the set of operations that make up required RM functionality. Access control for each operation must be considered during planning.

11.3. IT PROVIDER CONSIDERATIONS.

a. Required Roles.

There are several types of roles needed for performing RM functions as part of an IT solution. Personnel must understand how the roles will be filled for any IT system or service.

(1) End-point Role.

Human users and automation create and interact with data by executing business processes. Records are created and updated throughout the process, documenting that a decision was made, an event occurred, or a transaction was processed.

(a) Creators are end-point users who first generate the potential record.

(b) Editors are end-point users who have the ability to modify or edit a draft record.

(c) End-point users need access to update records and metadata appropriate to their business process role and their position in the organizations.

(d) End-point users are not allowed to dispose of records or remove them from government control.

(2) IT Technical Role.

Execution of system administration functions can help implement and can be affected by RM considerations. The IT provider must determine if this role is available to the customer for self-service or if the IT provider will fill this role. IT technical users:

(a) Require appropriate access to manage users and roles at the organization level.

(b) Are never authorized to remove or delete records without RM staff approval.

(c) Require access to sufficient information about how RM is implemented to answer questions about system or service use. Generally, this would be associated with a help desk function.

(3) RM Role.

(a) RM users are authorized to perform or approve RM activities that range from managing records schedule items to managing the records themselves. RM users:

1. May need to access or manage records from organic or non-organic RM tools, depending on the storage approach.

2. Can authorize or update some metadata fields and may apply and lift holds across their record collections.

3. Can additionally coordinate destruction for approval and execution.

(b) Machine or robotics users such as robotic process automation need appropriate access to collections and functions that allow proper management of records to fully exploit system or service APIs. This is important for using third party retention tracking and disposition management tools where records are managed in place or in a shared archive. Machine-to-machine access is constrained to specific activities approved by RM staff.

b. Multiple Customers.

IT systems or services with multiple customers may have to leverage shared resources. Vendor assumptions about deployment can affect access for RM staff who manage multiple collections of records across an organization's business and mission programs. To meet restrictions on cross-customer information access, IT providers should provide:

(1) Clear expectations on the support staff and products customers will receive for review and approval of centralized RM activities like retention control item creation and management or disposition.

(2) Service desk support to fulfill RM activity requests from the customer.

c. Automation Roles and Permissions.

Automation may act in any of the user roles from end-point users to RM to administrative users as long as access is authorized. Automation can be used for repetitive tasks such as applying defaulted information to created information, capturing dates of routine processes, or conducting patterns of business use on data to inform records managers handling the organizations records schedule.

d. Other Internal Controls.

Other users and permission may be needed for additional controls. These could be used:

(1) To support audits.

(2) For searches across the organization and across records collections.

11.4. OUTCOMES.

Table 13 enumerates a set of outcomes for IT systems and services to be used to assess implementation of the Access Control building block to support RM.

Table 13. Access Control Outcomes

ID	Outcome
08.01	IT system or service prevents unauthorized access or disposal of records.
08.02	IT system or service prevents unauthorized copy or removal from government custody.
08.03	IT system or service enables authorized users to grant access to information to another user or group of users for a predetermined time period.

Table 13. Access Control Outcomes, Continued

ID	Outcome
08.04	IT system or service provides RM functions, including records schedule update, rescheduling, holds, transfer, destruction, and reporting, to authorized RM users.
08.05	IT system or service automates repetitive RM and other activities such as tracking retention, identifying duplication, or performing analytics.
08.06	IT system or service enables and manages machine-to-machine access for RM users using a non-organic or third-party mechanism for managing records in the system or services.

SECTION 12: REPORTING AND METRICS

12.1. OVERVIEW.

a. RM oversight is supported through collecting and analyzing metrics and reporting the results to governing boards and oversight groups.

b. IT providers are accountable for making metrics visible to customers to configure for reporting requirements. Customers communicate metrics to IT providers and integrate metrics from all services into a consolidated RM status.

c. Reports support visibility and compliance to DoD policy and Federal statutes and regulations.

12.2. REQUIRED INPUTS.

a. Customer Reporting Requirements.

Any requirements for reporting RM activity and status must be identified and used as a baseline for reporting functionality.

b. Policy.

DoDI 5015.02 establishes the policy for the DoD Records Management Program and includes applicable guidance for IT systems and services.

c. Information About the DoD Strategic Plans.

The DoD seeks to improve information sharing and availability, assure security, identify efficiencies, and shorten IT deployment time. It also seeks to leverage AI to analyze information value and use. These strategic focus areas may affect how retention of records and information is planned and managed.

12.3. IT PROVIDER CONSIDERATIONS.

a. IT providers report the RM status of their system or service in the DoD Information Technology Portfolio Repository (DITPR).

b. RM reports will be available from the IT system or service for documenting destruction, transfer, holds, and other RM information. Logs of actions and metrics should be kept to support the reports.

c. RM may require consolidation of information from many systems into a dashboard or routine scorecard report that includes information about total records holdings related to the systems or services managing them.

12.4. OUTCOMES.

Table 14 enumerates a set of outcomes for IT systems and services to be used to assess implementation of the Reporting and Metrics building block to support RM.

Table 14. Reporting and Metrics Outcomes

ID	Outcome
09.01	RM status is reported to the DITPR.
09.02	IT system or service captures destruction manifests, plans, and reports that include the number of records destroyed, their topics, dates, and authorizations to support annual reporting to NARA and other stakeholders.
09.03	IT system or service captures permanent records transfer plans, manifests, successful receipts, topics, dates, and authorizations and reports to support annual reporting to NARA.
09.04	IT system or service captures logs of changes, reviews, and approvals, including rescheduling and hold actions.
09.05	IT system or service logs changes of location and responsible parties of record sets to support records inventory management.
09.06	IT supports formatting, printing, and saving reports from searches and logs that are legible, professional in appearance, and support the customer’s mission processes.

SECTION 13: RM OUTCOMES CHECKLIST

13.1. OVERVIEW.

The checklist (Table 15) consolidates the required outcomes introduced throughout this manual. The outcomes include compliance with NARA's Universal ERM Requirements and unique DoD requirements and support assessment processes. For each outcome:

a. A discussion of the benefits of meeting the outcome provides context within the checklist.

b. Columns highlight the need for approval by both the IT provider and the records staff. While not all outcomes will require both approvals, it is critical that these two stakeholders collaborate and agree on the RM planning artifacts.

13.2. USING THE CHECKLIST.

a. Use by IT Providers.

This checklist provides a framework for any IT provider to learn and understand RM considerations that are necessary for planning an IT system or service that will comply with DoDI 5015.02.

(1) Roadmap for Design Team.

The checklist can also be used as a roadmap into the material detailed in this issuance. It may be that different staff are responsible for different architectural components of the IT system or service. This list of outcomes related to their component will help them find appropriate guidance in this issuance.

(2) Guide for Stakeholder Collaboration.

The checklist guides the IT provider on whom to include in various activities. ROs must be present for many of the planning tasks, particularly during retention planning. When there are several customers of the IT system or service, there are key points identified for when customer input is needed.

b. Use by Assessors.

This checklist provides a tool for DoD and third-party organizations to assess compliance to DoDI 5015.02 by an IT system or service.

c. Use by Records Staff.

This checklist can be a vehicle for records staff to engage IT staff on ERM considerations. A key obstacle to realizing efficiencies of ERM is the translation needed between RM vocabulary and concepts to the world of IT and development, security, and operations.

Table 15. Compliance Checklist

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
01.01	Retention Planning	DoD IT system or service is identified as either purpose-built or utility.	Characterizes the data and may allow for default retentions.		
01.02	Retention Planning	Any records schedule items conflicts are identified and resolved or addressed.	Identifies need for vendors, IT providers, and customers to deconflict		
01.03	Retention Planning	Data retention plan (completed according to Paragraph 4.4.b.) defines the data managed by the IT system or service and the required characteristics of the data.	Identifies data groupings managed by the IT system or service and characterizes retention requirements.		
01.04	Retention Planning	IT system or service manages multiple dispositions and retention periods assigned to a single record or a record set.	Allows for multiple uses of the record and possible holds.		
01.05	Retention Planning	IT system or service clearly marks and protects unscheduled records from destruction or spoilage until NARA approves disposition.	Lowers risk of records loss and identifies follow up for records managers.		
01.06	Retention Planning	IT system or service provides the capability for authorized staff to define, load, and manage records schedules.	Enables electronic disposition assignments and change management to retentions.		
01.07	Retention Planning	IT system or service automatically applies changes to records schedules to affected records and information.	Automates updates of connection between records and retentions.		
01.08	Retention Planning	IT system or service supports position-based retention if required in the data retention plan.	Allows legal removal of low value information. Provides mechanism for timely disposition.		
01.09	Retention Planning	IT system or service supports GRS as defined in the data retention plan.	Saves time as GRS records schedule items are approved for use.		
01.10	Retention Planning	IT system or service creates or receives and manages digitized records schedule items for use within that IT system or service in accordance with existing DoD data and architecture standards.	Supports information exchange and trustworthiness in long term record retention tracking.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
02.01	Metadata	Metadata structures and sources are identified based on the disposition and use of the data groupings in the data retention plan.	Ensures that all metadata are available to manage tracking and disposition.		
02.02	Metadata	RM metadata plan is completed according to Table 7 defining the metadata requirements, sources, and additional characteristics.	Ensures metadata needed for RM, discovery, and other uses are included in IT.		
02.03	Metadata	Business rules for harvesting metadata are documented as part of the metadata plan. Purpose-built systems automatically assign metadata relevant to the supported business processes. Utility systems automatically assign metadata in accordance with organization's defaults and policies.	Lowers burden on end-point users. Improves control over entire data set. Improves accuracy and consistency of records.		
02.04	Metadata	IT system or service includes unique identification metadata to support retention management, finding and updating, access control, reporting, and disposal.	Enables tracking through the lifecycle and improves trust in responding to requests for information.		
02.05	Metadata	IT system or service assigns default, inherited, or harvested metadata values with the ability for humans to overwrite when appropriate.	Helps keep context complete and consistent. Reduces load on end-point users.		
02.06	Metadata	IT system or service incorporates metadata into or links metadata to the content or data.	Ensures accuracy and completeness and is required for electronic records control.		
02.07	Metadata	IT system or service keeps metadata synchronized.	Avoids duplication of metadata. Authoritative hosts of metadata should be identified and enforced.		
02.08	Metadata	IT system or service exchanges metadata using a standard format registered in the DISR.	Supports data sharing, interoperability, and maintenance.		
02.09	Metadata	Additional metadata to support business and organization policy, processes, and procedures is identified and documented in the RM metadata plan as appropriate.	Provides understanding during planning of structures needed for metadata. Allows optional population at identified points in lifespan.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
03.01	Capture	IT system or service clearly and visibly identifies finalized records.	Allows end-point users to remove non-records when authorized.		
03.02	Capture	IT system or service harvests and assigns metadata upon save, send, or receipt of data.	Allows for automated identification of initial assignment of identification metadata.		
03.03	Capture	IT system or service assigns disposition or event plan metadata harvested from environment, via defaults or from end-point user selecting pick list item.	Enables the automation of linking the data to its records schedule.		
03.04	Capture	IT system or service calculates and assigns the record designation date for temporary and permanent records.	Completes capture and identifies when the information is under records control and may trigger retention.		
03.05	Capture	IT system or service harvests and assigns the Office of Record or other entity accountable for disposal to all captured information.	Identifies metadata and assigns responsibility for ongoing management.		
03.06	Capture	IT system or service identifies essential records status.	Enables COOP processes.		
03.07	Capture	IT system or service harvests and applies exemptions and exclusions for purposes of FOIA and Privacy Act compliance.	Enables discovery activities while complying with applicable disclosure statute.		
03.08	Capture	IT system or service provides an industry standard mechanism for accepting records from external automation.	Enables bulk upload to create information and records within the IT system or service.		
03.09	Capture	IT system or service automatically populates metadata to uploaded or ingested records and information.	Enables bulk upload to create information and records within the IT system of service.		
03.10	Capture	IT system or service enforces immutability of temporary or permanent record content.	Complies with requirement for records to be immutable per law.		
04.01	Storage	Storage plan definition includes the technical approach for records storage, metadata storage, and any needed linking across the lifespan of the records.	Aids in identification of IT system or service requirements to enable any needed replacements.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
04.02	Storage	IT system or service maintains trustworthiness of the record and its associated metadata across storage architectures and strategies.	Meets records requirements if lifespan of record is longer than that of the IT system or service.		
04.03	Storage	Storage architecture protects set of essential records needed for COOP.	Enables COOP.		
04.04	Storage	IT system or service plans for storage of the record and its associated metadata for the required lifespan of the records as defined by their retentions.	Identifies additional requirements for storage or for transfer to other storage IT.		
05.01	Find & Update	IT system or service enables authorized users to search content and metadata of the records regardless of file type or encryption.	Meets requirements for records discovery.		
05.02	Find & Update	IT system or service provides the option for search results to be presented in the order of relevance to the search term.	Supports key automated discovery processes.		
05.03	Find & Update	IT system or service enables delegation or reassignment of a search request to trusted agents, including any data produced from that search to designated personnel for authorized business purposes.	Supports key automated discovery processes.		
05.04	Find & Update	IT system or service enables authorized users (including automation) to access and update record content.	Supports authorized access for viewing and updating across the lifespan of the record.		
05.05	Find & Update	IT system or service enables authorized users (including automation) to update or assign metadata to records, including retention codes, as they mature and are used.	Enables ERM processes.		
05.06	Find & Update	IT system or service enables authorized users (including automation) to update or assign metadata to records, including retention codes, as they mature and are used.	Allows for identification of authoritative sources and changes to their governance.		
05.07	Find & Update	IT system or service allows RM users to designate records be placed in a “hold” status and destruction ceased regardless of assigned retention.	Supports records holds processes.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
05.08	Find & Update	IT system or service allows RM users to release the “hold” designation of a record.	Supports records holds processes.		
05.09	Find & Update	IT system or service allows RM users to save and share searches.	Supports RM processes.		
06.01	Disposition: Destroy	IT system or service identifies records that are eligible for destruction.	Enables automated records processes.		
06.02	Disposition: Destroy	IT system or service uses an automated or workflow process to destroy those records eligible for destruction.	Enables automated records processes.		
06.03	Disposition: Destroy	IT system or service completes destruction of electronic records in a manner that protects any sensitive, proprietary, or national security information.	Enables automated records processes that comply with safeguarding guidance.		
06.04	Disposition: Transfer to NARA	IT system or service retains a copy of all permanent electronic records transferred to NARA until receiving official notification that NARA has accepted legal custody of the records.	Enables automated records transfer for preservation.		
06.05	Disposition: Transfer to NARA	IT system or service removes or disables passwords or other forms of file-level encryption that prevent access to records before transfer to NARA.	Enables automated records transfer for preservation.		
06.06	Disposition: Transfer to NARA	IT system or service transfers permanent records to NARA in the preferred and acceptable formats in accordance with NARA Bulletin 2015-04.	Enables automated records transfer for preservation.		
07.01	Maintain	IT system or service maintains records in findable and readable formats regardless of the life of the system.	Meets requirement for ERM for ongoing discovery and use of the records.		
07.02	Maintain	IT system or service supports publishing information in a digital format using a web-based interface for public facing systems and services.	Meets NARA requirement.		
07.03	Maintain	IT system or service ensures that records and associated metadata are not encrypted in a manner that obstructs access by operational controls for audits or responding to legal requests for information.	Meets NARA requirement.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
07.04	Maintain	IT system or service imports records and associated metadata maintaining relationships and record retention status.	Enables compliant import of data and records.		
07.05	Maintain	IT system or service exports records and associated metadata maintaining relationships and record retention status.	Enables compliant export of data and records.		
07.06	Maintain	IT system or service provides artifacts for imports and exports to be validated.	Enables compliant import and export of data and records.		
08.01	Access Control	IT system or service prevents unauthorized access or disposal of records.	Enables records control.		
08.02	Access Control	IT system or service prevents unauthorized copy or removal from government custody.	Enables records control.		
08.03	Access Control	IT system or service enables authorized users to grant access to information to another user or group of users for a predetermined time period.	Enables RM and discovery processes.		
08.04	Access Control	IT system or service provides RM functions including records schedule update, rescheduling, holds, transfer, destruction, and reporting to authorized RM users.	Enables ERM processes.		
08.05	Access Control	IT system or service automates repetitive RM and other activities such as tracking retention, identifying duplication, or performing analytics.	Enables ERM processes.		
08.06	Access Control	IT system or service enables and manages machine-to-machine access for RM users using a non-organic or third-party mechanism for managing records in the system or services.	Enables ERM processes.		
09.01	Reporting and Metrics	IT system or service reports RM status to the DITPR.	Meets requirements for DoDI 5015.02 compliance.		

Table 15. Compliance Checklist, Continued.

ID	Building Block	Requirement	Benefits	IT Provider Approval	Customer Approval
09.02	Reporting and Metrics	IT system or service captures destruction manifests, plans, and reports that include the number of records destroyed, their topics, dates, and authorizations to support annual reporting to NARA and other stakeholders.	Supports RM processes.		
09.03	Reporting and Metrics	IT system or service captures permanent records transfer plans, manifests, successful receipts, topics, dates, and authorizations and reports to support annual reporting to NARA.	Supports RM processes.		
09.04	Reporting and Metrics	IT system or service captures logs of changes, reviews, and approvals including rescheduling and hold actions.	Supports RM processes.		
09.05	Reporting and Metrics	IT system or service logs changes of location and responsible parties of record sets to support records inventory management.	Supports RM processes.		
09.06	Reporting and Metrics	IT system or service supports formatting, printing, and saving reports from searches and logs that are legible, professional in appearance, and support the customer's mission processes.	Supports RM processes.		

SECTION 14: REQUIRED FUNCTIONALITY FOR RM CAPABILITY

14.1. RM OPERATIONS PROVIDE A USER PERSPECTIVE.

a. This list of RM operations provides a view into RM functionality that is useful for development purposes, testing purposes, and user understanding.

b. RM operations are enabled by the outcomes documented in this issuance. If an IT system or service meets all of the listed outcomes, the RM operations will be available.

14.2. REQUIRED RM OPERATIONS.

a. For each RM operation, Table 16 includes considerations for the IT provider as planning for the IT system or service is underway.

b. For each RM operation, the possible roles that may have responsibility for executing that operation are listed. For each IT system or service, the responsibility for executing each RM operation must be documented.

Table 16. Required RM Functionality

RM Operation	Considerations for IT Provider	Execution Responsibility
Create, edit, and delete data	Records and potential records	End-point user
Find and retrieve data	Customer's organizational policies may restrict finding and retrieving permissions based on valid authorization, proper need-to-know, non-disclosure agreement, or other criteria	End-point user
Manually assign records schedule items to data	• Must be assigned from a defined list • Assignment overrides any storage location or system-wide defaults	End-point user
Finalize records	When finalized, permission to delete is removed, revisions are versioned	End-point user
Audit data	• Actions are logged • Recommended for customer responsibility	• Records custodian • Records manager • IT customer technical staff • IT provider technical RM support staff

Table 16. Required RM Functionality, Continued

RM Operation	Considerations for IT Provider	Execution Responsibility
Change records schedule item assignment on finalized records	• Actions are logged • Recommended for customer responsibility	• Records custodian • Records manager • IT customer technical staff • IT provider technical RM support staff
Search and retrieve across all data including those in safe harbor	• Actions are logged • Recommended for customer responsibility when necessary to support electronic discovery	• Records custodian • Records manager • IT customer technical staff • IT provider technical RM support staff
Delete non-finalized versions of data in their custody	• Actions are logged • Recommended for customer responsibility	• Records custodian • Records manager • IT customer technical staff • IT provider technical RM support staff
Create, find, retrieve, audit, and manage records schedule items	Actions are logged	• Records manager • IT customer technical staff • IT provider technical RM support staff
Make records schedule items available for assignment.	Actions are logged	• Records manager • IT customer technical staff • IT provider technical RM support staff
Execute disposal actions including coordinating disposition reviews and reporting.	Actions are logged	• Records manager • IT customer technical staff • IT provider technical RM support staff
Define, apply, and lift holds	• Actions are logged • Applying and lifting holds may be delegated to a records custodian	• Records manager • IT customer technical staff • IT provider technical RM support staff
Execute transfer actions for a defined set of data	Actions are logged	• Records manager • IT customer technical staff • IT provider technical RM support staff

Glossary

G.1. ACRONYMS.

Acronym	Meaning
AI	artificial intelligence
API	application programming interface
CFR	Code of Federal Regulations
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COOP	continuity of operations
DD	Department of Defense (form)
DISR	DoD Information Technology Standards Registry
DITPR	DoD Information Technology Portfolio Repository
DoDD	DoD directive
DoDI	DoD instruction
ERM	electronic records management
FOIA	Freedom of Information Act
GRS	General Records Schedule
IE	information enterprise
ISO	International Organization for Standardization
IT	information technology
NARA	National Archives and Records Administration
PDF	portable document format
RM	records management
RO	records officer
SF	standard form
TIFF	Tagged Image File Format
XML	Extensible Markup Language

G.2. DEFINITIONS.

TERM	DEFINITION
access control	The process of granting or denying specific requests for obtaining and using information and related information processing services.
administrative records	Defined in DoDI 5015.02.
Artifact	An architectural work product that describes an aspect of the architecture.
Capstone	An approach where disposition instructions of emails are based on senior officials designated by account level or by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function in accordance with GRS 6.1.
Capture	The process of placing an object under RM control for disposition and access purposes. Objects are not necessarily moved from the system they reside in when they are captured. Records can be imported from other sources, manually entered into the system, or linked to other systems.
cloud storage	A pooled, on demand, configurable storage resource provided on-demand that can be rapidly provisioned and released with minimum management efforts or service provider interaction.
Customer	An organization that pays for an IT system or service, whether internally or externally acquired or shared.
Curation	The identification, assessment and contextualizing of records to facilitate management across the records' lifespan from capture through disposition.
Data	A representation of facts, concepts or instructions, such as text, numbers, graphics, documents, images, sound or video, in form suitable for communication, interpretation or processing, which individually have no meaning by and in themselves.
data ingestion	A process of obtaining and importing data for immediate use.
data retention plan	An artifact listing the data managed in an IT system or service and specific characteristics about the data needed to inform the acquisition and development for RM purposes.

TERM DEFINITION

data warehouse A storage architecture designed to hold data extracted from transaction systems, operational data stores, and external sources. The warehouse then combines that data in an aggregate, summary form suitable for enterprise-wide data analysis and reporting for predefined business needs.

Disposition Those actions taken regarding records no longer needed for the conduct of the regular current business of the agency.

disposition authority The legal authorization for the retention and disposal of records represented as an alphanumeric code.

disposition review The process for gaining approval for records destruction, ranging in formality from pre-approval for automatic disposition to sign off on individual records by the accountable authority.

DoD IE The DoD information resources, assets, and processes required to achieve an information advantage and to share information across DoD and with mission partners. It includes:

The information itself and DoD management over the information life cycle.

The processes, including risk management, associated with managing information to accomplish the DoD mission and functions.

Activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise.

Related information resources such as personnel, funds, equipment, and IT, including internal use software and national security systems.

electronic records Defined in DoDI 5015.02.

Encryption The process of changing plaintext into ciphertext for the purpose of security or privacy.

end-point users Organization staff members or automation that interact directly with IT to perform a business function including compliance and oversight. End-point users may be restricted to view only access, but for the purposes of RM, they are assumed to create data.

essential records Defined in DoDI 5015.02.

TERM **DEFINITION**

event disposition A disposition instruction in which a record is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention period is applied and there is no fixed waiting period as with “timed” or combination “timed-event” dispositions. Example: “Destroy upon completion of Government Accountability Office Audit”.

file plan A subset of the organization’s records schedules that includes a listing of records schedule items that apply to the office.

GRS Schedules issued by the Archivist of the United States to provide disposition authority for records common to several or all agencies of the Federal Government. These schedules authorize agencies, after specified periods of time, to either destroy temporary records or transfer permanent records to NARA.

Hold A designation to cease disposition of data until further notice. Holds can be used for legal, audit, review, or other purposes.

Immutability The state of being not subject or susceptible to change.

information product A set of electronically stored information.

IT provider An organization supplying systems or services to one or more internal or external customers.

IT service An IT capability designed to provide awareness of, access to, and delivery of data or information made available for consumption by one or more users. Users can be an individual, organization, or machine.

IT system Complementary networks of hardware and software that people and organizations use to collect, filter, process, create, and distribute data.

IT vendor The last entity in the chain that brands an IT product and sells it directly to end users or through a channel. An IT vendor may design and manufacture its own products, assemble complete systems from components produced by others, or procure products from an original equipment or contract manufacturer. An IT vendor may also provide services or maintenance for its own products or for other vendors’ products.

TERM DEFINITION

intermediary records Records created or used in the process of creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or financial obligations or to initiate, sustain, evaluate, or provide evidence of decision making.

interoperability Defined in DoDI 5015.02.

manage in place Electronic records are stored and managed within the IT system or service in which they are created or received.

Metadata Literally, "data above 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.

metadata schema Organizing structure for metadata that often includes standards for common components such as dates, names, and places. Metadata schemas can be discipline specific to enable interoperability.

national security system Defined in Section 3552(b)(6) of Title 44, United States Code.

non-record information Defined in DoDI 5015.02.

permanent records Federal records that have been determined by NARA to have sufficient value to warrant their preservation in the National Archives.

potential record Data in its beginning form that is being managed by the IT system or service but is not yet known to be a record.

purpose-built IT IT systems and services designed for a specific business or mission purpose, and the records created or managed in the IT system or service and their retentions can be identified during design time.

position-based retention A means of managing and scheduling records and information where final disposition is determined by the role or position of the account user, rather than the value of the content. An example of this approach applied to email is GRS 6.1.

Record Defined in DoDI 5015.02.

TERM **DEFINITION**

records custodian An organizational staff member who is charged with coordinating and enforcing hands-on records and information management for about 20 to 100 end-point users. They respond to tasking from records managers and ROs for support in inventory, auditing, disposition reviews, and reporting. Generally, this is an office manager or administrative assistant as delegated by the commander or director. If RM is provided as a service, this could be an IT person who executes previously defined actions on behalf of a service customer.

record designation date Date that the record is declared final (e.g., cutoff, publication, creation) and starts the retention period that will be used to calculate the disposition date based on the records schedule item. ("Date [Creation Date]" as required for permanent records in accordance with NARA Bulletin 2015-04.)

RM Defined in DoDI 5015.02.

records manager An organization staff member who is accountable for executing an organization's records and information program, including coordinating destruction and transfer reviews and retention holds.

RM operation RM-related tasks that a user may execute as part of their responsibilities.

RO The designated individual who has the authority to certify records schedules and submit them to NARA for their organization.

records schedule Means any of the following:

(1) A Standard Form 115, Request for Records Disposition Authority that has been approved by NARA to authorize the disposition of Federal records;

(2) A GRS issued by NARA; or

(3) A published agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more SF 115s or issued by NARA in the GRS.

records schedule item A line item of a records schedule that includes a description of a set of records with an associated disposition authority that has been scheduled and approved by NARA.

TERM **DEFINITION**

reference data Data used to organize or categorize other data (e.g., controlled values), or for relating data to information (e.g., calibration data) both within and beyond the boundaries of the enterprise. Usually consists of codes and descriptions or definitions.

retention period The length of time that records must be kept.

retention planning The process of documenting the DoD information and its ongoing value to the business or mission that will be created or managed by the IT system or service. This information includes groups of data, associated records schedule items, their sources, accountable information owners, and responsible stewards for the data housed in each system or service.

safe harbor A period after destruction of information is requested, to allow for recovery of that information without any loss of content, metadata, or state.

temporary record A record that has been determined to have insufficient value (on the basis of current standards) to warrant its preservation by NARA. A temporary record has a non-permanent retention.

time disposition A disposition instruction that begins the fixed retention period at a specific point in time. Example: "Destroy after 2 years — cut off at the end of the calendar (or fiscal) year; hold for 2 years; then destroy".

time-event disposition A disposition instruction specifying that a record shall be disposed of at a fixed period of time after a predictable or specified event. Once the specified event has occurred, then the retention period is applied. Example: "Destroy 3 years after close of case." The record does not start its retention period until after the case is closed — at that time its folder is cutoff and the retention period (destroy after 3 years).

Transfer The moving of the custody of records from one organization to another, which may or may not involve change of location, control, or legal ownership.

transitory records Routine records required only for a short time and that are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision making.

undeclared records Data groupings that have not been identified as records or potential records.

TERM	DEFINITION
unscheduled records	Records whose final disposition have not been approved by NARA. Such records must be treated as permanent until a final disposition is approved.
utility IT	IT system and service that generates data to be used for many business or mission purposes and will have a variety of business or mission values.
workspace	Physical or virtual area where work is accomplished. Virtual workspaces include the ability to create, store, share, edit, and destroy digital work products.

REFERENCES

Chairman of the Joint Chiefs of Staff Manual 5760.01A, Vol. II 0500 Series, "Joint Staff and Combatant Command Records Management Manual: Volume II—Disposition Schedule" July 13, 2012

Code of Federal Regulations, Title 36, Chapter XII, Subchapter B

Directive-Type Memorandum-22-001, "DoD Standards for Records Management Capabilities in Programs Including Information Technology," March 3, 2022, as amended

DoD Chief Information Officer Memorandum, "DoD Artificial Intelligence Strategy," June 27, 2018

DoD Chief Information Officer Memorandum, "DoD Data Strategy," September 30, 2020

DoD Chief Information Officer Memorandum, "DoD Records Strategy," (coming by 26 Dec)

DoD Chief Information Officer Memorandum, "Federated Data Catalog - Minimum Metadata Requirements", October 10, 2021.

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016 as amended

DoD Instruction 3020.42, "Defense Continuity Plan Development", February 17, 2006

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," October 2012

Intelligence Community Technical Specification, "XML Data Encoding Specification for Electronic Records Management," July 29, 2016

International Organization for Standardization 14721:2012, "Space Data and Information Transfer Systems - Open Archival Information System (OAIS) - Reference Model"

International Organization for Standardization 15489-1:2016, "Information and Documentation - Records Management - Part 1: Concepts and Principles"

International Organization for Standardization 23081-2:2009, "Information and Documentation - Managing Metadata for Records - Part 2: Conceptual and Implementation Issues"

National Archives and Records Administration, "General Records Schedule," https://www.archives.gov/records-mgmt/grs

National Archives and Records Administration, "General Records Schedule 5.2 Transitory and Intermediary Records," https://www.archives.gov/records-mgmt/grs

National Archives and Records Administration, "General Records Schedule 6.1 Email Managed under a Capstone Approach," https://www.archives.gov/records-mgmt/grs

National Archives and Records Administration, "Universal Electronic Records Management (ERM) Requirements," https://www.archives.gov/records-mgmt/policy/universalermrequirements

National Archives and Records Administration Bulletin 2014-02, "Guidance on Managing Social Media Records," October 24, 2013

National Archives and Records Administration Bulletin 2015-04, "Metadata Guidance for the Transfer of Permanent Electronic Records," September 15, 2015

National Institute of Standards and Technology, Special Publication 800-145, "The NIST Definition of Cloud Computing," September 2011

National Information Exchange Model Executive Steering Council, "National Information Exchange Model," current edition

Office of the Program Manager, Information Sharing Environment, "Priority Objective 3: Data Tagging Functional Requirements," Version 1.0, December 2014

United States Code, Title 5, Sections 552 and 552a (also known as the "Freedom of Information Act" and "Privacy Act", respectively)

United States Code, Title 44, Section 3552(b)(6)