InterPARES Project

International Research on Permanent Authentic Records in Electronic Systems

Documents Mapping InterPARES Authenticity Requirements Against Existing Standards

InterPARES Project

International Research on Permanent Authentic Records in Electronic Systems

Appendix 14.1

Mapping of InterPARES Authenticity Task Force Benchmark Requirements for Authenticity Version 2.1 (May 2001) Against Provisions ISO/DIS 15489 Draft International Standard: Records Management (May 2000)

Prepared for the Authenticity Task Force by
Associate Professor Sue McKemmish
Australian Team
June 2001

Background

This report was prepared at the request of the Authenticity Task Force Chair. It maps the Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records contained in the Draft Requirements for Authenticity Version 2.1 (May 2001) against the provisions in ISO/DSI 15489 Draft International Standard: Records Management (May 2000).

The Benchmark Requirements developed by the Authenticity Task Force specify "the evidence provided in association either with the records, the electronic system or the administrative procedure that supports the preserver's inference of the authenticity of the creator's electronic records".

Scope of ISO

As specified in Section 1 of the Draft ISO, the standard provides guidance on managing records of originating organizations, public or private, for internal and external clients, but not on the management of archival records within archival institutions. ISO/DSI 15489 applies to the management of records, in all formats or media, created or received by any public or private organization in the conduct of its activities, or any individual with a duty to create and maintain records. It provides guidance on determining the responsibilities of organizations for records and records policies, procedures, systems and processes, and provides guidance on records management in support of a quality process framework to comply with ISO9001, ISO9002 and ISO14001. The intended audience for the standard is made up of:

- managers of organizations
- records, information and technology management professionals
- all other personnel in organizations
- other individuals with a duty to create and maintain records.

According to Section 4 of the draft standard, records management in an organization includes:

- setting policies and standards;
- assigning responsibilities and authorities;
- establishing and promulgating procedures and guidelines;
- providing a range of services relating to the management and use of records;
- designing, implementing and administering specialized systems for managing records; and
- integrating records management into business systems and processes.

Section 6 Policy and Responsibilities deals generally with establishing policies in relation to all aspects of records management. Sections 6.1-6.3 specify that organizations should establish, document, maintain and promulgate policies, procedures and practices for records management, the objective of which should be the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. Records management policy and responsibilities should be endorsed at the highest level of decision making, and promulgated, communicated and implemented at all levels in the organization. Responsibility for compliance should be assigned to all employees of the organization, including records managers, allied information professionals, executives, business unit managers, systems administrators and others who create records as part of their work, and should be reflected in job descriptions and similar statements. Specific leadership responsibility and accountability for records management should be assigned to a person with appropriate authority within the organization.

Section 7.2 of the Draft ISO specifies broadly that records management policies, procedures and practices should lead to authoritative records which have the characteristics of authenticity (7.2.1), reliability (7.2.2), integrity (7.2.3), and useability (7.2.4).[1]

Purpose of Mapping

As both the Benchmark Requirements developed by the InterPARES Authenticity Task Force and the Draft ISO deal with the authenticity of records in creating organizations, it would seem useful to determine the degree of correspondence between the Benchmark Requirements and Draft ISO provisions:

- as an input into the review and discussion of the Benchmark Requirements
- as an input into consideration of strategies relating to incorporating the findings of the InterPARES project into existing/evolving standards in the records and archives field.

In particular the following map may assist the Authenticity Task Force in determining answers to the following questions:

- What is the relationship between the Benchmark Requirements for Authenticity and the provisions of the Draft ISO?
- How far do they overlap?

[1] The draft ISO defines authenticity, reliability, integrity and useability in the following terms:

> An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported.
> A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
> The integrity of a record refers to its being complete and unaltered.
> A useable record is one that can be located, retrieved, presented and interpreted.

- If records creators were to comply with the provisions of the Draft ISO, would their policies, procedures, processes, systems, and records meet the Benchmark Requirements for Authenticity?

A detailed mapping is provided on the following pages. My tentative conclusions from the mapping are presented in the following table:

Table 1:
Summary Chart Mapping InterPARES Requirements Against Provisions of ISO Records Management Standard

The specified Benchmark Requirement	**Would be satisfied by compliance with the following Draft ISO Provisions**
REQUIREMENT A.1: Expression of Record Attributes and Linkage to Record	7.1 Principles of Records Management Programmes 7.2 Characteristics of Records 7.2.1 Authenticity 7.2.3 Integrity 9.3 Records Capture
REQUIREMENT A.2: Access Privileges	7.1 Principles of Records Management Programmes 7.2.1 Authenticity 7.2.3 Integrity 8.3 Designing and Implementing Records Systems 8.3.2 Documenting Records Transactions 8.3.6 Access, Retrieval and Use 8.3.7 Retention and Disposition 9.5.1 Classification of Business Activity 9.7 Access
REQUIREMENT A.3: Protective Procedures: Loss and Corruption of Records (Note: relate specifically and narrowly to backup procedures.)	8.2 Records Systems Characteristics 8.2.1 Reliability 8.2.2 Integrity 8.2.5 Systematic 8.3 Designing and Implementing Records Systems 8.3.2 Documenting Records Transactions 8.3.6 Access, Retrieval and Use 8.3.7 Retention and Disposition (Note: relate to a range of procedures and generally to backup processes.)

REQUIREMENT A.4: Protective Procedures: Media and Technology	8.3.3 Physical Storage and Management 8.3.5 Conversion and Migration 8.5 Discontinuing Records Systems 9.6 Storage and Handling
REQUIREMENT A.5: Establishment of Documentary Forms	7.1 Principles of Records Management Programmes 8.4 Design and Implementation Methodology
REQUIREMENT A.6: Authentication of Records	---
REQUIREMENT A.7: Identification of Authoritative Record	---
REQUIREMENT A.8: Removal and Transfer of Relevant Documentation	8.3 Designing and Implementing Records Systems 9.6 Storage and Handling 9.8 Tracking 9.9 Implementing Disposition 9.10 Documenting Records Management Processes

Table 2:
Detailed Mapping of InterPARES Requirements Against Provisions of ISO Records Management Standard

Benchmark Requirements[1]	Related Provisions of Draft International Standard ISO/DIS 15489 Records Management[2]
To support a presumption of authenticity the preserver must obtain evidence that:	
REQUIREMENT A.1:	
Expression of Record Attributes and Linkage to Record the value of the following attributes are explicitly expressed and inextricably linked to every record. These attributes can be distinguished into categories, the first concerning the identity of records, and the second concerning the integrity of records. A.1.a: identity of the record: A.1.a.i: Names of the persons concurring in the formation of the record (that is, the names of the author, writer, addressee, originator) A.1.a.ii: Name of action or matter A.1.a.iii: Date (that is, document, archival and transmission dates) A.1.a.iv: Expression of archival bond (for	Sections 7.1 Principles of Records Management Programmes, 7.2 The Characteristics of a Record and 9.3 Records Capture include provisions which relate to this requirement. Section 7.1 includes relevant provisions relating to: • determining what records should be created in each business process, and what information needs to be included in the records; • deciding in what form and structure records should be created and captured, and the technologies to be used; • determining what metadata should be created with the record and through records processes and how that metadata will be persistently linked and managed; • determining requirements for retrieving, using and transmitting records between business processes and other users and how long they need to be kept to satisfy those requirements.

[1] InterPARES Project, "Draft Requirements for Authenticity", Version 2.1, May 2001

[2] ISO TC 46/SC11 N253, *ISO/DIS 15489 Draft International Standard: Records Management, 2000-05-29*

example, classification code, file identifier) A.1.a.v: Indication of attachments A.1.b: integrity of the record: A.1.b.i: Name of handling office A.1.b.ii: Name of office of primary responsibility (if different from handling office) A.1.b.iii: Indication of types of annotations added to the record A.1.b.iv: Indication of technical modifications The presumption of a record's authenticity is strengthened by knowledge of certain basic facts about it. The attributes identified in this requirement embody those facts. The requirement that the attributes be expressed explicitly and linked inextricably to the record during its life, and carried forward with it over time and space, reflects the Task Force's belief that such expression and linkage provide a strong foundation on which to	Section 7.2 specifies broadly that records management policies, procedures and practices should lead to authoritative records which have the characteristics of authenticity (7.2.1), reliability (7.2.2), integrity (7.2.3), and useability (7.2.4).[1] In relation to authenticity (7.2.1), it states that organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment. In relation to integrity (7.2.3) it states that a record must be protected against unauthorized alteration and that therefore records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions, or annotations may be authorized, and who is authorized to make them. It also specifies that any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

[1] The draft ISO defines authenticity, reliability, integrity and useability in the following terms:
An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; to have been created or sent at the time purported.
A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
The integrity of a record refers to its being complete and unaltered.
A useable record is one that can be located, retrieved, presented and interpreted.

[2] The Draft ISO defines metadata as data describing context, content and structure of records and their management through time (3.12).

[3] Classification is defined in the Draft ISO as the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system (3.5).

establish a record’s identity and demonstrate its integrity. The case studies undertaken as part of the work of the Task Force revealed very little consistency in the way the attributes that specifically establish the identity of a record are captured and expressed from one electronic system to another. In certain systems, some attributes were explicitly mentioned on the face of the record, in others they could be found in a wide range of metadata linked to the record or they were simply implicit in one or more of the record’s contexts. In many cases, certain attributes (for example, the expression of the archival bond) were not captured at all. The Task Force’s concern is that, in the absence of a precise and explicit statement of the basic facts concerning a record’s identity and integrity, it will be necessary for the preserver to acquire enormous, and otherwise unnecessary, quantities of data and documentation simply to establish those facts.

The link between the record and the core information is viewed by the Task Force as a conceptual rather than a physical one, and the requirement could be satisfied in different ways, depending on the nature of the electronic system in which the record resides. For example, in electronic records management systems, this requirement is

Section 7.2 further specifies that, as well as the content, the record should contain, or be persistently linked to, or associated with, the metadata necessary to document a transaction, as follows:

a) the structure of a record, that is, its format and the relationships between the elements comprising the record, should remain intact;
b) the business context in which the record was created, received and used should be apparent in the record (including the business process of which the transaction is part, the date and time of the transaction and the participants in the transaction);
c) the links between documents, held separately but combining to make up a record, should be present.

This part of Section 7.2 is complemented by Section 9.3 which deals with “records capture”, i.e. a process involving

a) establishing a relationship between the record, the creator and the business context that originated it;
b) the placement of the record and its relationship within a records system;
c) the linking of the record to other records.

Section 9.3 specifies that the allocation of explicit metadata,[2] embedded in, attached to or associated with, the specific record, irrespective of its format, should be designed into the procedures of a records system. It states that such metadata is essential for re-tracing, with authority, the status, structure and integrity of the record at any particular time and demonstrating its relationships with other records. It defines the following techniques to ensure capture of records:

- registration (9.4) which assigns a unique identifier within the system to the record and provides evidence of the existence of records in a records system;

usually met through the creation of a record profile. In other types of systems, the requirement could be fulfilled through a topic map. A topic map expresses the characteristics (that is, topics) of subjects (for example, records or record attributes) and the relationships between and among them. When a record is exported from the live system, migrated in a system update, or transferred to the preserver, the attributes should be linked to the record and available to the user. When pulling together the data prior to export, the creator should also ensure that the data captured are the right data. For example, in the case of distribution lists, the creator must ensure that if the recipients specified on 'List A' were changed at some point in the active life of records, the accurate 'List A: Version 1' is exported with the records associated with the first version, and that the second version is sent forward with those records sent to recipients on 'List A: Version 2.'	• classification[3] and indexing (further specified in section 9.5) which enable appropriate linkages to provenance and other records, grouping, naming, security protection, user permissions and retrieval, disposition, and identification of vital records; • arrangement in a logical structure and sequence, whether a physical file or an electronic directory, which facilitates subsequent use and reference; and • systems which profile or template the actions undertaken in doing business, which o provide metadata describing the business context, o provide evidence of where a record is located, o identify what action is outstanding, o identify who has accessed a record, o identify when such access took place, and o provide evidence of the transactions that have been undertaken on the record.
REQUIREMENT A.2: Access Privileges the creator has defined and effectively implemented access privileges concerning the creation, modification,	Section 7.2 Characteristics of Records, especially 7.2.1 and 7.2.3 (see above for detail), relate to this requirement. Section 9.7 Access specifies organizations should have formal guidelines

annotation, relocation, and destruction of records;

Defining access privileges means assigning responsibility for the creation, modification, annotation, relocation and destruction of records on the basis of competence, which is the authority and capacity to carry out an administrative action. Implementing access privileges means conferring exclusive capability to exercise such responsibility. In electronic systems, access privileges are usually articulated in tables of user profiles. Effective implementation of access privileges involves the monitoring of access through an audit trail that records every interaction that an officer has with each record (with the possible exception of viewing the record). If the access privileges are not embedded within the electronic system but are based on an external security system (such as the exclusive assignment of keys to a location), the effective implementation of access privileges will involve monitoring the security system.

regulating who is permitted access to records and in what circumstances. It states that an access status should be assigned to both records and individuals, and that:

a) records are categorized according to their access status at a particular time;
b) records are only released to those who are authorized to see them;
c) encrypted records can be read as and when required and authorized;
d) records processes and transactions are only undertaken by those authorized to perform them; and
e) parts of the organization with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

Section 9.5.1 Classification of Business Activities recommends classification as a tool to assist in a range of records management processes including determining security protection and access appropriate for sets of records, and allocating user permissions for access to or action on particular groups of records.

Section 8.3 Designing and Implementing Records Systems contains the following provisions relating to audit procedures:

- Records systems should contain complete and accurate representations of all transactions that occur in relation to a particular record. These include the processes associated with individual records. Such details may be documented as part of the metadata embedded in, attached to, or associated with, a specific record. Alternatively they may be recorded as audit trails which should be kept at least as long as the document to which they relate is retained (8.3.2 Documenting Records Transactions).

	• Systems should include and apply controls on access to ensure that the integrity of the records is not compromised. They should provide and maintain audit trails or other methods to demonstrate that records were effectively protected from unauthorized use, alteration or destruction (8.3.6 Access, Retrieval and Use). • Records systems should be capable of facilitating and implementing decisions on the retention or disposition of records. It should be possible for these decisions to be made at any time in the existence of records, including in the design stage of records systems. It should also be possible, where appropriate, for disposition to be activated automatically. Systems should provide audit trails or other methods to track completed disposition actions (8.3.7 Retention and Disposition).
Requirement A.3: Protective Procedures: Loss and Corruption of Records the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records; Procedures to protect records against loss or corruption include: prescribing regular backup copies of records and their attributes; maintaining a system backup that includes system programs, operating system files, etc.; maintaining an audit trail of additions and changes to records since the last periodic backup; ensuring that, following any system	Section 8.2 Records Systems Characteristics specifies the characteristics a records systems should have in order to support records that have the characteristics of authenticity, reliability, integrity, and useability. The specifications include the following relevant requirements: • Any system deployed to manage records should be capable of continuous and regular operation in accordance with responsible procedures (8.2.1 Reliability). • A records system should protect the records from unauthorized alteration or disposition (8.2.1 (c)). • The reliability of the system should be documented by creating and maintaining records of systems operation (8.2.1). • Control measures such as access monitoring, user verification, authorized destruction and security should be implemented to prevent unauthorized access, destruction, alteration or removal of

failure, the backup and recovery procedures will automatically guarantee that all complete updates (records and any control information such as indexes required to access the records) contained in the audit are reflected in the rebuilt files and also guarantee that any incomplete operation is backed up. The capability should be provided to rebuild forward from any backup copy, using the backup copy and all subsequent audit trails.	records. These controls may reside within a records system or be external to the specific system. For electronic records, the organization may need to prove that any system malfunction, upgrade or regular maintenance does not affect the records' integrity (8.2.2 Integrity). • Records should be created, maintained and managed systematically. Records creation and maintenance practices should be systematized through the design and operation of both records systems and business systems (8.2.5 Systematic). • A records system should have accurately documented policies, assigned responsibilities and formal methodologies for its management (8.2.5). The audit provisions in 8.3 Designing and Implementing Records Systems (see above) are also relevant to this Requirement. (Note: relate to a range of procedures and generally to backup processes.)
REQUIREMENT A.4: Protective Procedures: Media and Technology the creator has established and implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change; Procedures to counteract media fragility and	Section 8.3 Designing and Implementing Records Systems includes the following relevant provisions: • Appropriate storage environment and media, physical protective materials, handling procedures and storage systems should be considered when designing the records system. Knowing how long the records will need to be kept and maintained will affect decisions on storage media. The records system should address disaster preparedness to ensure that risks are identified and mitigated. Integrity should be demonstrably maintained during and after

technological obsolescence include: planning upgrades to the organisation’s technology base; ensuring the ability to retrieve, access and use stored records when components of the electronic system are changed; refreshing the records by regularly moving them from one storage medium to another; and migrating records from an obsolescent technology to a new technology.	recovery from disaster (8.3.3 Physical Storage Medium and Protection). • Records systems should be designed so that records will remain authentic, reliable and useable throughout any kind of system change, including format conversion, migration between hardware and operating systems or specific software applications, for the entire period of their retention (8.3.5 Conversion and Migration). Section 8.5 Discontinuing Records Systems specifies that when a records system is discontinued or decommissioned, no further records may be added to the system, although they should continue to be accessible. Records may be removed from the system in accordance with retention and disposition guidelines in force, or with conversion and migration strategies. The process of discontinuing systems should be documented as such detail will be required to maintain the authenticity, reliability, useability and integrity of records still held within that system, including conversion plans or data mapping. Section 9.6 Storage and Handling specifies that records should be stored on media that ensure their useability, reliability, authenticity and preservation for as long as they are needed. It states that issues relating to the maintenance, handling and storage of records arise throughout their existence, not only when they become inactive. Related provisions in 9.6 include: • Records require storage conditions and handling processes that take into account their specific physical and chemical properties. • Records of continuing value, irrespective of format, require higher quality storage and handling to preserve them for as long as that value exists.

- Storage conditions and handling processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.
- Organizations should have policies and guidelines for converting or migrating records from one records system to another.
- Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention. This may include migration to different software, re-presentation in emulation formats or any other future ways of re-presenting records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.

REQUIREMENT A.5:
Establishment of Documentary Forms
the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator;

The documentary form of a record may be determined in connection to a specific administrative procedure, or in connection to a specific phase(s) within a procedure. The documentary form may be prescribed by workflow control technology, where each step in an administrative procedure is identified by

Section 7.1 Principles of Records Management Programmes includes relevant provisions relating to:

- determining what records should be created in each business process, and what information needs to be included in the records;
- deciding in what form and structure records should be created and captured, and the technologies to be used;
- determining what metadata should be created with the record and through records processes and how that metadata will be persistently linked and managed.

Section 8.4 Design and Implementation Methodology specifies how to conduct an analysis of business activity, involving the identification of each business function, activity and transaction, and the identification of related requirements for records with reference to the organisation’s

specific record forms. If a creator customises a specific application, such as an electronic mail application, to carry certain fields the customised form becomes, by default, the required documentary form. It is understood that the creator, either acting on the basis of its own needs, or the requirements of the juridical system, not an individual officer, establishes the required documentary form(s) of records. When the creator establishes the documentary form in connection to a procedure, or to specific phases of a procedure, it is understood that this includes the determination of the intrinsic and extrinsic elements of form that will allow for the maintenance of the authenticity of the record. Because, generally speaking, that determination will vary from one form of a record to another, and from one creator to another, it is not possible to predetermine or generalise the relevance of specific intrinsic and extrinsic elements of documentary form in relation to authenticity.	regulatory environment. It also specifies that it is necessary to determine: • how each requirement may be satisfied through records management processes • the records structure which best satisfies each function, activity or transaction. Section 8.4 also specifies that records management processes and records systems should be designed and implemented with a view to integrating the operation of records systems with business processes and related systems.
REQUIREMENT A.6: Authentication of Records if authentication is required by the juridical system or the needs of the organization, the	No specifications relate directly to authentication processes.

creator has established specific rules regarding which records must be authenticated, by whom, and the means of authentication;	
REQUIREMENT A.7: Identification of Authoritative Record if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative;	No specifications relate directly to this requirement.
REQUIREMENT A.8: Removal and Transfer of Relevant Documentation if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator has established and implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records. This requirement implies that the creator needs to carry forward with the removed records all the information that is necessary	Section 9.8 Tracking[1] deals in general with movement and location tracking in records systems to: a) identify outstanding action required; b) enable retrieval of a record; c) prevent loss of records; d) monitor usage for systems maintenance and security, and maintain an auditable trail of records transactions (i.e. capture or registration, classification, indexing, storage, access and use, migration and disposition); and e) maintain capacity to identify the operational origins of individual records where systems have been amalgamated or migrated. 9.8.3 deals specifically with Location Tracking and states that the movement of records should be documented to ensure that items can always be located

[1] Defined in the Draft ISO as creating, capturing and maintaining information about the movement and use of records (3.19).

to establish the identity and demonstrate the integrity of those records. If the system is designed to generate a profile for each record that expresses all the attributes identified in Requirement A.1 it is sufficient to remove the profiles with the records. In the absence of such a profile, it may be necessary to remove and transfer with the records audit trails, indexes, data directories, data dictionaries, and so on.	when required. It further states that tracking mechanisms record the item identifier, the title, the person or unit having possession of the item and the time/date of movement; and that the system should track the issue, transfer between persons, and return of records to their 'home' location or storage as well as their disposition or transfer to any other authorized external organization including an archives authority. Section 9.9 Implementing Disposition contains the following relevant provisions: • Disposition authorities which govern the removal of records from operational systems should be applied to records on a systematic and routine basis, in the course of normal business activity. No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation or investigation is current or pending which would involve relying on the record as evidence. • Disposition action may encompass: o immediate physical destruction, including overwriting and deletion; o retention for a further period within the business unit; o transfer to an appropriate storage area or medium under organizational control; o transfer to another organization that has assumed responsibility for the business activity through restructure, sale or privatisation; o transfer to a storage area managed on behalf of the organization by an independent provider where appropriate contractual arrangements have been entered into;

[1] In the Draft ISO, disposition action includes records retention, destruction and transfer (3.9). Transfer is defined as both a change of custody, ownership and/or responsibility for records, and the movement of records from one location to another (3.20 and 3.21).

- transfer of responsibility for management to an appropriate authority while physical storage of the record is retained by the creating organization;
- transfer to an organizational archive; or
- transfer to an external archives authority.

Section 9.10 Documenting Records Management Processes specifies that all decisions on which records should be captured and how long records should be maintained should be clearly documented and retained. Decisions may be presented as a disposition authority. Formal documentation of the analysis or other assessment that results in decisions to capture and retain records should be prepared and submitted to senior management for approval. The documentation should contain details of business activities and the records that result from each business activity, and specify their retention periods and disposition actions clearly and unambiguously. Events that activate or enable disposition actions[1] should be clearly identified. Instructions for the transfer of records to alternative forms of storage (e.g. off-line or off-site storage) should be included. Where necessary, such documentation should be submitted to an external authorising body, such as an archival authority, auditors, etc. for necessary approval. A record of disposition actions, once they have been carried out, should be maintained.

The audit provisions in 8.3 Designing and Implementing Records Systems, and the provisions of Section 9.6 Storage and Handling (as detailed above) are also relevant to this Requirement.

InterPARES Project

International Research on Permanent Authentic Records in Electronic Systems

Appendix 14.2

Mapping of InterPARES Authenticity Requirements Against Provisions of DoD 5015.2 Records Management Standard

Prepared for the Authenticity Task Force by
Ian McAndrew
University of British Columbia
August 2001

Background

The *Design Criteria Standard for Electronic Records Management Software Applications* was a product of the collaborative research that took place in 1995 and 1996 between the United States Department of Defense Records Management Task Force and the “UBC Project” [The Preservation of the Integrity of Electronic Records]. The standard is more commonly know as *DoD 5015.2*.

The purpose of the DoD standard is to prescribe “mandatory baseline functional requirements, and [to] identif[y] non-mandatory features deemed desirable for Records Management Application (RMA) software.”[1]

Because 5015.2 was originally created for use by agencies of the United States government, the standard is designed and expressed in terms of compliance with U.S. laws and regulations. However, it can be regarded as an international standard to an extent due to the fact that it can be, and has been, adapted for use in other nations.

Within the context of its use by the U.S. government, 5015.2 is a procurement standard: that is, government agencies purchasing RMAs are required to ensure that software packages they install are compliant with, at least, the minimum specifications as outlined in Chapter 2 (and, for systems containing security classified records, those outlined in Chapter 4, section C4.1). Agencies have the option of selecting among several off-the-shelf software packages certified as 5015.2-compliant by the Defense Information Systems Agency.

Scope and structure of DoD 5015.2

As a result of its genesis within the DoD-UBC Project collaboration, it is fair to say that 5015.2 is firmly based on archival science and records management theory. Accordingly, many of its features promote practices that function toward guarding the authenticity of records. However, it would be inaccurate to suggest that there is any overt emphasis on authenticity issues in the standard.

Note as well that the DoD standard is written with the perspective of records creators in mind. Thereby, only a few 5015.2 provisions can be understood as being parallel to the stipulations of InterPARES Requirement Set B, and, when relationships of this sort do occur, they tend to be incidental.

The standard is structured as follows:

Chapter 1: General Information
Chapter 2: Mandatory Requirements
Chapter 3: Non-Mandatory Features

[1] 5015.2 Standard, “C1.1. Purpose.”

Chapter 4: Management of [Security] Classified Records
Appendix: Definitions

Throughout the standard, paragraphs and individual requirements are assigned alpha-numeric codes incorporating chapter number and further subdivisions. For example, “C2.1” refers to Chapter 2, first section; “C2.2.3.6” refers to Chapter 2, second section, third sub-section, sixth paragraph/requirement; “AP1.8” refers to the eighth definition in the Appendix. Please note that all references in this document to individual paragraphs/requirements indicate the alpha-numeric code associated with the paragraph/requirement, and please keep in mind when making reference to tables below that:

a) any item preceded by an alpha-numeric code beginning with “C3” is a non-mandatory feature; and
b) any item preceded by an alpha-numeric code beginning with “C4” is only applicable to those systems containing security classified records.

The main body of the standard is presented in Chapter 2, which lists mandatory requirements. In order to provide a sense of major topics covered, the principal subdivisions of Chapter 2 are listed below:

C2.2.1. Implementing File Plans
C2.2.2. Scheduling Records
C2.2.3. Declaring and Filing Records
C2.2.4. Filing Electronic Mail Messages (E-mail)
C2.2.5. Storing Records
C2.2.6. Retention and Vital Records Management
C2.2.7. Access Control
C2.2.8. System Audits
C2.2.9. System Management Requirements
C2.2.10. Additional Baseline Requirements

Note that there is considerable overlap between these categories. For example, provisions related to access control appear not just in section C2.2.7, but in six of the other sections of Chapter 2 as well.

Presumptions underlying DoD 5015.2

The following presumptions are embedded in the DoD standard:

1. that 5015.2-compliant RMAs will be implemented within the larger context of a hybrid (electronic – non-electronic) records system

As consequence of this presumption, some of the particular requirements of 5015.2 pertain to features necessary for electronic management of non-electronic records. This is mainly achieved by requiring system functionality to enable agencies to create and manage electronic profiles for all records, including those created using traditional media. Note, however, that the standard does not cover any matters outside the electronic system that would be necessary to implement hybrid records management, such as organizational procedures.

2. that agencies may have “site-specific needs”[1] which will not be met by implementation of an RMA compliant only with the mandatory requirements

Chapter 3, pertaining to “Non-Mandatory Features,” is included to accommodate those situations wherein agencies recognize that satisfying the “minimum records management requirements”[2] contained in Chapter 2 will not be sufficient. In addition, Chapter 2 has been drafted such that it allows agencies with site-specific needs to require further functionalities than those set out as minimum requirements. For example, paragraph/requirement C2.2.7.1. stipulates that

> The RMA, in conjunction with its operating environment, shall use authentication measures that allow only authorized persons access to the RMA. *At a minimum*, the RMA will implement authentication measures that require:
> **C2.2.7.1.1.** Userid.
> **C2.2.7.1.2.** Password.

3. that RMAs will feature hierarchical classification systems

The language used to describe the features of the classification system envisioned within 5015.2 is distinctive—and indeed somewhat confusing—and thus it requires some explanation here. First, it appears that the principal tool used to define and implement the classification system is the “file plan,” which is defined as “a document containing the identifying number, title, description, and disposition authority of files held or used in an office.”[3] Second, within the classification system it appears that there are two levels of record aggregates: file plan components and record folders (“A record folder is an extension to the file plan either as a static structure or an aggregate gathering of records. It is used to manage case records and to break other records into periods supporting retention and disposition”[4]).

[1] 5015.2 Standard, “C1.2. Limitations.”

[2] 5015.2 Standard, “C1.1. Purpose.”

[3] 5015.2 Standard, “AP1.43. File Plan.”

[4] 5015.2 Standard, “AP1.65. Record Folder.”

In any given instance there may be several aggregates within each of these aggregate categories. For instance, it seems that a record might be classified within a sub-folder; the sub-folder within a folder; the folder within a second-level file plan component; and this subsidiary component within a primary-level file plan component. It may be appropriate to suggest, as an analogy, that file plan components are roughly equivalent to series and sub-series, and that record folders are approximate counterparts to files and folders.

Note that the DoD standard makes certain requirements regarding classification levels and metadata. First, there are metadata attributes that must be linked with record aggregates in addition to those that must be associated with records. Second, there are mandatory ‘linkages’ and ‘associations’ between records and the various kinds of aggregations.

However, note that the standard is somewhat unclear on these issues. For one matter, 5015.2 appears to use ‘link’ and ‘associate’ as synonyms, and fails to define either term. Thereby, it is not possible to ascertain the character of the physical, logical, or intellectual relationships between, for instance, a record and the metadata associated with the aggregates to which it belongs. Second, the standard refers to “identifiers” and “components” associated with both file plans and record folders without defining either term, or making clear how they relate to each other. The dilemma here is that terms are used ambiguously. For example, “file plan component” seems to be used to refer to both record aggregates, as described above, and to metadata elements (see C2.2.1.1. for an example). All of which is simply to re-emphasize that the interpretation of the DoD vision for a classification system presented here is highly speculative due to the ambiguity of the document itself.

Introduction to this document

This document maps the latest version of the InterPARES Authenticity Requirements[1] against the 5015.2 standard[2] for the purpose of demonstrating similarities and differences between them. There are currently three versions of the DoD standard available on the website of the Department of Defense Joint Interoperability Test Command: a draft version, dated August 1995; the version currently in force, dated November 1997; and a draft-revision version dated June 2001. This document treats the 2001 version of the standard.

The body of this report is comprised by three main tables. The first is a Summary Table that lists InterPARES Authenticity Requirements alongside citations to parallel provisions in the standard. This is included here to allow quick reference for those already familiar with DoD 5015.2. The following table maps InterPARES Requirements against provisions of 5015.2, presenting the same data as in Table

[1] “Draft for Public Comment” version, 31 July 2001.
[2] See “RMA Certification Testing Home Page,” <http://jitc.fhu.disa.mil/recmgt/>

1 but including full text of the DoD requirements, as opposed to citations only. Table 3 provides further detail on those stipulations of the DoD standard related to InterPARES Requirement A.2 on access privileges. This aspect of the mapping has been carried forward into a separate table simply due to the fact that such a large proportion of the 5015.2 standard deals with access privileges. There is also an appendix to this report which reproduces a table directly from 5015.2 in order to provide yet further details on access privileges within the standard.

Table 1:
Summary Chart Mapping InterPARES Requirements Against Provisions of DoD 5015.2 Records Management Standard

Table 1 provides a summary of the InterPARES-DoD 5015.2 mapping. InterPARES Requirements are listed in the left-hand column, and citations to parallel passages from 5015.2 are provided in the right-hand column.

InterPARES Requirement	DoD 5015.2 Citation
REQUIREMENT SET A	
REQUIREMENT A.1: Expression of Record Attributes and Linkage to Record	C2.2.3.10. C2.2.3.20.
A.1.a: identity of the record:	
A.1.a.i: Names of persons	C2.2.3.2.9. C2.2.3.2.10. C2.2.3.2.11.
A.1.a.ii: Name of action or matter	C2.2.3.2.3.
A.1.a.iii: Date (that is, document, archival and transmission dates)	C2.2.3.2.6. C2.2.3.2.7. C2.2.3.2.8.
A.1.a.iv: Expression of archival bond (for example, classification code, file identifier)	C2.2.3.2.1. C2.2.1.1.1. C2.2.1.1.2. C2.2.1.1.3. C2.2.1.3.1. C2.2.1.3.1.1. C2.2.1.3.1.2.
A.1.a.v: Indication of attachments	No counterpart for Requirement A.1.a.v has been identified.

A.1.b: integrity of the record:	
A.1.b.i: Name of handling office	
A.1.b.ii: Name of office of primary responsibility (if different from handling office)	C2.2.3.2.12.
A.1.b.iii: Indication of types of annotations added to the record	No counterpart for Requirement A.1.b.iii has been identified.
A.1.b.iv: Indication of technical modifications	No counterpart for Requirement A.1.b.iv has been identified.
REQUIREMENT A.2: Access Privileges	C2.2.5.1. C2.2.7.1. C2.2.7.1.1. C2.2.7.1.2. C2.2.7.3. C2.2.3.14. C2.2.8.1. C2.2.8.4. C2.2.8.7. C2.2.8.7.1. C2.2.8.7.2. C2.2.8.7.3. C2.2.8.7.4. C2.2.8.7.5. C4.1.16.
REQUIREMENT A.3: Protective Procedures: Loss and Corruption of Records	C2.2.3.8. C2.2.3.9. C2.2.5.2. C2.2.8.4. C2.2.9.1. C2.2.9.2. C2.2.9.3. C2.2.9.4. C2.2.9.5.
REQUIREMENT A.4: Protective Procedures: Media and Technology	C2.1.4. C2.2.9.6. C2.2.10.3. C3.1.1.

REQUIREMENT A.5: Establishment of Documentary Forms	C2.2.1.2. C2.2.3.4. C2.2.3.7. C2.2.3.12. C2.2.3.24.
REQUIREMENT A.6: Authentication of Records	No counterpart for Requirement A.5 has been identified.
REQUIREMENT A.7: Identification of Authoritative Record	C2.2.3.17. C2.2.3.18. C2.2.3.19.
REQUIREMENT A.8: Removal and Transfer of Relevant Documentation	C2.2.3.20. C2.2.6.5.2. C2.2.6.5.3. C2.2.6.5.4. C2.2.10.4. C2.2.10.5.
REQUIREMENT SET B The preserver should be able to demonstrate that:	
REQUIREMENT B.1: Controls over Records Transfer, Maintenance, and Reproduction	C2.2.6.5.1.. C2.2.6.5.2. C2.2.10.5. C2.2.5.2. C2.2.10.3.
REQUIREMENT B.2: Documentation of Reproduction Process and its Effects	C2.2.8.4. C3.2.12. C3.2.12.1. C3.2.12.2. C3.2.12.3. C3.2.12.4. C3.2.12.5.
REQUIREMENT B.3: Archival Description	No counterpart for Requirement B.3 has been identified.

Table 2:
Detailed Mapping of InterPARES Requirements Against Provisions of DoD 5015.2 Records Management Standard

Table 2 presents the detailed mapping of the InterPARES Requirements against provisions of DoD 5015.2. InterPARES Requirements are listed in the left-hand column, and full text of parallel passages in 5015.2 are provided in the middle column. Note that the extent to which stipulations from the two documents match precisely differs in each case: in some instances the cited DoD provisions entirely fulfill the InterPARES Requirement they are listed beside; in other instances they do so only partially. Comments are provided, when relevant, in the left-hand column to explain the rationale for mapping decisions made in those cases where it might not be clear precisely how the cited DoD provision relates to the InterPARES Requirement in question. Additionally, note when 5015.2 requirements can be identified as parallel to more than one InterPARES Requirement, they are listed in all applicable locations.

InterPARES Requirement	DoD 5015.2 Provision	Comments
REQUIREMENT SET A To support a presumption of authenticity the preserver must obtain evidence that:		
REQUIREMENT A.1: Expression of Record Attributes and Linkage to Record the value of the following attributes are explicitly expressed and inextricably linked to every record. These	C2.2.3.10. RMAs shall (for all records) capture or provide the user with the capability to populate the metadata elements before filing the record. RMAs shall ensure that fields designated mandatory for data collection are non-null before filing the record. C2.2.3.20. RMAs shall link the record metadata to the record so that it can be accessed for display,	

attributes can be distinguished into categories, the first concerning the identity of records, and the second concerning the integrity of records.	export, etc.	
	[Note: all elements listed below are designated as mandatory in DoD 5015.2][1]	
A.1.a: identity of the record:		
A.1.a.i: Names of the persons concurring in the formation of the record (that is, the names of the author, writer, addressee, originator)	C2.2.3.2.9. Author or Originator C2.2.3.2.10. Addressee(s) C2.2.3.2.11. Other Addressee(s)	“Addressee” defined as “The name of the organization to which or individual to whom a record is addressed.” [See AP1.3.] Other terms not defined.
A.1.a.ii: Name of action or matter	C2.2.3.2.3. Subject or Title	“Subject” defined as “The principal topic addressed in a record.” [See AP1.80.] “Title” not defined.

[1] Also note that a special metadata set is specified for capture in the case of e-mail records. This set includes all elements required for records in general, as well as: the intelligent name of the sender [“Intelligent names are clear, uncoded, identifications of the individual.”]; the intelligent name of all primary addressees (or distribution lists); the intelligent name of all other addressees (or distribution lists); the date and time the message was sent; for messages received, the date and time the message was received (if available); the subject of the message. Furthermore, note that an additional 18 elements are mandated for capture in the case of records classified for security purposes.

A.1.a.iii: Date (that is, document, archival and transmission dates)	C2.2.3.2.6. Date Filed C2.2.3.2.7. Publication Date C2.2.3.2.8. Date Received		“Date Filed” defined as “ The date and time that an electronic document was filed in the RMA and thus became a record. This date and time will normally be assigned by the computer at the time the record is filed in the RMA.” [See AP1.19.] Publication Date” defined as “ The date and time that the author or originator completed the development of or signed the document. For electronic documents, this date and time should be established either by the author or from the time attribute assigned to the document by the application used to create the document. This is not necessarily the date or time that the document was filed in the RMA and thus became a record.” [See AP1.59.] Date received” not defined.

A.1.a.iv: Expression of archival bond (for example, classification code, file identifier)	Record metadata: C2.2.3.2.1. Unique Record Identifier File plan metadata: C2.2.1.1.1. Record Category Name C2.2.1.1.2. Record Category Identifier C2.2.1.1.3. Record Category Description Record folder metadata:[1] C2.2.1.3.1. Record Folders C2.2.1.3.1.1. Folder Name C2.2.1.3.1.2. Folder Unique Identifier	"Record Identifier" defined as "An element of metadata, a record identifier is a data element whose value is system-generated and that uniquely identifies a particular record." [See AP1.66.] "Record Category Identifier" defined as "An agency's alphanumeric or numeric identifier indicating a unique record category." [See AP1.64.] "Record Folder" defined as "A record folder is an extension to the file plan either as a static structure or an aggregate gathering of records. It is used to manage case records and to break other records into periods supporting retention and disposition." [See AP1.65.] Other terms not defined.

[1] While the 5015.2 standard is somewhat unclear on the matter, it appears that each record is linked to the appropriate record folder, and its metadata, and to the appropriate file plan and its metadata. The standard specifies as follows: that "RMAs shall provide the capability to associate the attributes of one or more record folder(s) to a record [C2.2.3.1.];" that "each [record folder] component identifier shall be linked to its associated [record folder] component and to its higher-level file plan component identifier(s) [C2.2.1.3.];" and that "each component identifier shall be linked to its associated component and to its higher-level component identifier(s) [C2.2.1.1.]."

A.1.a.v: Indication of attachments	No counterpart for Requirement A.1.a.v has been identified.	
A.1.b: integrity of the record:		
A.1.b.i: Name of handling office **A.1.b.ii:** Name of office of primary responsibility (if different from handling office)	C2.2.3.2.12. Originating Organization	"Originating organization" defined as "Official name or code identifying the office responsible for the creation of a document." [See AP1.57.] This does not precisely match any person defined by InterPARES. Thus, depending on how it is interpreted, its closest counterpart in InterPARES terminology could be handling office ["the office that is formally competent for carrying out the action to which the record relates or for the matter to which the record pertains"]; or office of primary responsibility ["the office given the formal competence for maintaining the original (or official) records belonging to a given class within the integrated classification scheme and retention schedule"].[1]

A.1.b.iii: Indication of types of annotations added to the record	No counterpart for Requirement A.1.b.iii has been identified.	
A.1.b.iv: Indication of technical modifications	No counterpart for Requirement A.1.b.iv has been identified.	
REQUIREMENT A.2: Access Privileges the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records; Note: See table that follows for further details on access privileges in DoD 5015.2.	C2.2.5.1. RMAs shall provide an interface to one or more repositories for storing electronic records. The RMAs shall prevent unauthorized access to the repository(ies). C2.2.7.1. The RMA, in conjunction with its operating environment, shall use authentication measures that allow only authorized persons access to the RMA. At a minimum, the RMA will implement authentication measures that require: C2.2.7.1.1. Userid. C2.2.7.1.2. Password. C2.2.7.3. RMAs shall provide the capability to define different groups of users with different access privileges. RMAs shall control access to file plan components, record folders, and records based on group membership as well as user account information. At a minimum, access shall be restricted to appropriate portions of the file plan for purposes of filing and/or searching/retrieving.	Requirements from C2.2.8.1 to C4.1.16 pertain to "the monitoring of access through an audit trail that records every interaction that an officer has with each record." See 31 July 2001 draft of InterPARES Authenticity Requirements, Section 4, Subsection A.2.

C2.2.3.14. RMAs shall provide the capability for only authorized individuals to limit the record folders and record categories presented to a user or workgroup. Based on these limits, RMAs shall present to users only those record categories or folders available to the user or workgroup for filing.

C2.2.8.1. The RMA shall provide an audit capability to log the date, time, and user ID for actions performed on each record and associated metadata. These actions include: view, create, copy, delete, move, print, and edit actions.

C2.2.8.4. RMA audit utilities shall provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

C2.2.8.7. The following audit information shall be logged for each delete operation

- C2.2.8.7.1. Unique Record Identifier.
- C2.2.8.7.2. Unique Folder Identifier (if applicable).
- C2.2.8.7.3. Record Category Identifier.
- C2.2.8.7.4. User Account Identifier.
- C2.2.8.7.5. Date/Time.

C4.1.16. <u>Record History Audit</u>. The RMA shall capture and link an audit history of each record by

	capturing the replaced metadata value and the person who entered that value, and appending them to a record audit history file. The metadata fields to be captured shall be authorized individual selectable.	
Requirement A.3: Protective Procedures: Loss and Corruption of Records the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records;	C2.2.3.8. RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved C2.2.3.9. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable. C2.2.5.2. RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. C2.2.8.4. RMA audit utilities shall provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service. C2.2.9.1. Backup of Stored Records. The RMA system shall provide the capability to automatically create backup or redundant copies of the records.	There is no explicit requirement in DoD 5015.2 that audit trails must log all “additions and changes to records since the last periodic backup.” However, it is implied that RMAs must have such functionality in C2.2.9.5.

C2.2.9.2. Storage of Backup Copies. The method used to back up RMA database files shall provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful destruction.

C2.2.9.3. Scheduling of Backup Copies. The using organization shall schedule the backup copies and recycle or destroy the medium in accordance with the disposition schedule.

C2.2.9.4. Recovery/Rollback Capability. Following any system failure, the backup and recovery procedures provided by the system shall ensure data integrity by providing the capability to compile updates (records, metadata, and any other information required to access the records) to RMAs, ensure these updates are reflected in RMA files, and ensuring that any partial updates to RMA files are separately identified. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been attempted. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files.

C2.2.9.5. Rebuild Capability. The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system audit trails.

REQUIREMENT A.4: Protective Procedures: Media and Technology the creator has established and implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change;

C2.1.4. <u>Backwards Compatibility</u>. RMAs shall provide the capability to access information from their superceded repositories and databases. This capability shall support at least one previously certified version of backward compatibility.

C2.2.9.6. <u>Storage Availability and Monitoring</u>. The system shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data, and records. The system shall notify individuals of the need for corrective action in the event of critically low storage space.

C2.2.10.3. <u>Ability to Read and Process Records</u>. Since RMAs are prohibited (see paragraph C2.2.3.8.) from altering the format of stored records, the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by maintaining the hardware and software used to create or capture the record; by maintaining hardware and software capable of viewing the record in its native format; by ensuring backward compatibility when hardware and software is updated, or by migrating the record to a new

	format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record. C3.1.1. Storage Availability. The acquiring or using activity should define the size of the storage space required for its organizational records, along with the related record metadata and associated audit files.	
REQUIREMENT A.5: Establishment of Documentary Forms the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator;	C2.2.1.2. RMAs shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data. C2.2.3.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization. C2.2.3.7. RMAs shall provide the capability for authorized individuals to arrange record metadata components and user defined record components on data entry screens to be used for filing. C2.2.3.12. RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g. project number, budget line) for	These requirements function toward supporting Requirement A.5 because they establish a system configuration in which agencies will be able to “customise a specific application … to carry certain fields.” When this occurs, “the customised form becomes, by default, the required documentary form.” See 31 July 2001 draft of InterPARES Authenticity Requirements, Section 4, Subsection A.5.

	site-specific requirements. C2.2.3.24. RMAs shall provide the capability for users to create and maintain templates that automatically populate commonly used data into record metadata fields.
Requirement A.6: Authentication of Records if authentication is required by the juridical system or the needs of the organization, the creator has established specific rules regarding which records must be authenticated, by whom, and the means of authentication;	No counterpart for Requirement A.5 has been identified.

Requirement A.7: Identification of Authoritative Record if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative;	C2.2.3.17. RMAs shall provide the capability to link original superseded records to their successor records. C2.2.3.18. RMAs shall provide the capability to support multiple renditions of a record. These shall be associated and linked. C2.2.3.19. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions.	DoD 5015.2 includes no explicit requirement that the authoritative record be identified, nor any stipulation that the office of primary responsibility must be named in the retention schedule. However, requirements C2.2.3.17 through C2.2.3.19 establish fairly stringent rules for version control. The inclusion of these provisions might be taken to indicate that the standard implicitly requires identification of the authoritative record.
Requirement A.8: Removal and Transfer of Relevant Documentation if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the	C2.2.3.20. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc. C2.2.6.5.2. RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the records and metadata	The main relevant provisions here are the first three reproduced at left. Please note italicized words and phrases in these passages. The subsequent

electronic system, the creator has established and implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records.	shall be made to conform to one of the formats and media specified in 36 CFR 1228.270. C2.2.6.5.3. RMAs shall, for records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the metadata shall be made to conform to one of the formats and media specified in 36 CFR 1228.270. C2.2.6.5.4. RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed. RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned. C2.2.10.4. <u>Distribution Lists</u>. If the RMA is not able to access and store e-mail distribution lists from the e-mail server, the organization shall implement procedures to extract and store them as records. C2.2.10.5. <u>Accessioning Records to NARA</u>. When accessioning records and metadata to NARA, if conforming to formats and media specified in 36 CFR 1228.270 causes a violation of the records' authenticity and/or integrity, the organization should contact NARA for guidance	provisions are related less directly to the matter of supporting documentation to be transferred, but may be pertinent nevertheless.

REQUIREMENT SET B

The preserver should be able to demonstrate that:

REQUIREMENT B.1: Controls over Records Transfer, Maintenance, and Reproduction the procedures and system(s) used to transfer records to the archival institution or program, maintain them, and reproduce them embody adequate and effective controls to guarantee the records' identity and integrity, and specifically that	C2.2.6.5.1. RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession. C2.2.6.5.2. RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the records and metadata shall be made to conform to one of the formats and media specified in 36 CFR 1228.270[2]	While there are no overt provisions in 5015.2 pertaining to Requirement B.1 and its sub-requirements, procedures for transfer are fairly rigorous. The first three DoD requirements listed at left set the general framework for these procedures. Note also that there are requirements for the deletion and destruction of those records not selected for transfer as well. See

B.1.a: unbroken custody of the records is maintained; **B.1.b:** security and control procedures are implemented and monitored; and **B.1.c:** the content of the record remains unchanged after reproduction.	C2.2.10.5. Accessioning Records to NARA. When accessioning records and metadata to NARA, if conforming to formats and media specified in 36 CFR 1228.270 causes a violation of the records’ authenticity and/or integrity, the organization should contact NARA for guidance.	in particular items C2.2.5.3, C2.2.6.5.4, C2.2.8.7, C3.2.1, and sub-section C2.2.6.6. Furthermore, it may be the case that 5015.2 indirectly satisfies the InterPARES sub-requirements listed in association with B.1. First, while there is no provision making unbroken custody mandatory in 5015.2, section 1228.100 of the United States Code of Federal Regulations requires that “the Archivist of the United States and heads of Federal agencies are responsible for preventing the alienation or unauthorized destruction of records.” Thereby, presuming that “alienation” refers to a breach of custody, it

	C2.2.5.2. RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. C2.2.10.3. Ability to Read and Process Records. Since RMAs are prohibited (see paragraph C2.2.3.8.) from altering the format of stored records, the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by maintaining the hardware and software used to create or capture the record; by maintaining hardware and software capable of viewing the record in its native format; by ensuring backward compatibility when hardware and software is updated, or by migrating the record to a new format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record.	would seem that the standard need not address this matter since the law does so already. Second, the standard does not require “security and control procedures” in so many words, but, presumably these are built-in to the transfer mechanism by which records are copied to “a user-specified filename, path, or device.” Finally, while there are no stipulations requiring that the content of a record remain unchanged during the reproduction process, it may be that the standard simply does not differentiate between this particular kind of reproduction, and other kinds. If this is the case, it would seem that the final two items at left would serve to satisfy B.1.c to some

		extent at least.
REQUIREMENT B.2: Documentation of Reproduction Process and its Effects the activity of reproduction has been documented, and that this documentation includes **B.2.a:** the date of the records' reproduction and the name of the responsible person; **B.2.b:** the relationship between the records acquired from the creator and the copies produced by the preserver; **B.2.c:** the impact of the reproduction process on their form, content, accessibility and use; and	C2.2.8.4. RMA audit utilities shall provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service C3.2.12. Records Management Forms. An organization may determine that RMAs should have the capability to generate completed standard records management forms, such as: C3.2.12.1. Standard Form 115 and 115-A, "Request for Records Disposition Authority." C3.2.12.2. Standard Forms 135 and 135A, "Records Transmittal and Receipt." C3.2.12.3. Standard Form 258, "Request to Transfer, Approval, and Receipt of Records to the National Archives of the United States." C3.2.12.4. National Archives Form 14012, "Database Record Layout." C3.2.12.5. National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives."	C2.2.8.4 requires documentation of "transfer and destruction activities," although it does not deal with processes of reproduction per se. C3.2.12 has the potential to fulfill Requirement B.2. However, note that this provision is optional rather than mandatory. In addition, while it seems that the forms referred to in C3.2.12 might constitute documentation of the sort specified in B.2 [e.g., to judge from the title, "Technical Description for Transfer" sounds as if it might require data pertinent to B.2], it is unknown at this time precisely what information these forms capture.

B.2.d: in those cases where a copy of a record is known not to fully and faithfully reproduce the elements expressing its identity and integrity, such information has been documented by the preserver, and this documentation is readily accessible to the user.	
Requirement B.3: **Archival Description** the archival description of the fonds containing the electronic records includes–in addition to information about the records' juridical-administrative, provenancial, procedural, and documentary contexts–information about changes the electronic records of the creator have undergone since they were first created.	No counterpart for Requirement B.3 has been identified.

Table 3:
Detailed Provisions on Access Privileges Within DoD 5015.2 Records Management Standard

Altogether, the DoD standard defines four categories of access profiles: user, application administrator, records manager, and privileged user. In any given agency, presumably, there may be variation in specific access privileges granted to individuals assigned a given profile. For example, all records managers would be assigned a "records manager profile," but the specific access privileges defined for junior and senior records office staff would differ.

The standard does not address the matter of access profiles and privileges for users in great detail (see items listed as counterparts to InterPARES Requirement A.2 in Table 2). However, it does devote considerable attention to defining system requirements that relate to access privileges for application administrators, records managers, and privileged users. The following table provides a summary of these specifications.

The items are listed according to topical categories. However, since any given stipulation may relate to more than one topic, it should be understood that the way in which items are categorized below is open to challenge (i.e., the point of categorizing items was not to classify them, but simply to help in organizing the material). Also note that the stipulations that follow refer to "authorized individuals" when defining system requirements related to special access privileges for application administrators, and/or records managers, and/or privileged users. For further details on the differences between access privileges granted to each of these specific groups of authorized individuals, see Table 4.

Category	5015.2 citation
Access privilege specifications related to general and miscellaneous system functionalities	**C2.2.3.16.** RMAs shall provide a capability for referencing or linking and associating supporting and related records and related information, such as notes, marginalia, attachments, and electronic mail-return receipts, etc., to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations. **C2.2.6.7.1.** RMAs shall provide the capability for authorized users to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan. **C3.2.1. Making Global Changes.** RMAs should provide the capability for authorized individuals to make global changes to the record categories, record category identifiers, disposition instructions, disposition instruction identifiers, and originating organization. In addition, RMAs should provide the capability to

	reorganize the file plan and automatically propagate the changes resulting from the reorganization to the affected records and record folders. This capability includes managed deletion of records associated with deleted file plan branches. **C3.2.2. Bulk Loading Capability.** RMAs should provide the capability for authorized individuals to bulk load: **C3.2.2.1.** An Agency's pre-existing file plan. **C3.2.2.2.** Electronic records. **C3.2.2.3.** Record metadata.
Access privilege specifications related to security classification and declassification of records	**C4.1.9. Maintaining the Declassify On Time Frame.** RMAs shall provide the capability for authorized individuals to establish and maintain the period of time used to verify the “Declassify On” field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period. **C4.1.10. Classification Guides.** RMAs should provide a capability that allows an authorized individual to establish an automatically triggered classification mechanism. When a designated classification guide indicator is entered in the “Derived From” field, the following fields are automatically populated: **C4.1.10.1.** Reason(s) for Classification. **C4.1.10.2.** Initial Classification. **C4.1.10.3.** Declassify On. **C4.1.15. Exemption Categories.** RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the “Declassify On” field. **C4.1.20.** The RMA shall provide a capability whereby authorized users restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include: **C4.1.20.1.** Current Classification (C4.1.1.2.). **C4.1.20.2.** Supplemental Marking List (C2.2.2.2.2.). **C4.1.20.3.** Metadata Elements identified by the organization to be used for access control. **C4.2.1.** RMAs should provide the capability to allow authorized user selected metadata fields to be provided their own classification.
Access privilege specifications	**C2.2.8.2.** The RMA shall provide a capability whereby an authorized individual can determine which of the specified

related to administration of audit trails	actions listed in C2.2.8.1. are audited. **C2.2.8.3.** The RMA, in conjunction with its operating environment, shall provide a query function whereby an authorized individual can set up specialized reports to determine what level of access a user has, what records each user accessed, and what operations were performed on those records and associated metadata. These operations include view, create, copy, delete, move, print, and edit. **C2.2.8.6.** The following audit information shall be reported on demand to authorized individuals: **C2.2.8.6.1.** Total Number of Records. **C2.2.8.6.2.** Number of Records by Record Category Identifier. **C2.2.8.6.3.** Number of Accesses by Record Folder Identifier. **C2.2.8.6.4.** Number of Accesses by Record Identifier. **C2.2.8.6.5.** Date and Time Record Metadata modified and user ID by Record Identifier. **C2.2.8.8.** RMAs shall allow only authorized individuals to backup and remove audit files from the system. **C4.1.17. <u>Using the Record History Audit</u>.** The RMA shall provide the capability to view, copy, save, and print the record history file based on user permissions; shall not allow the editing of the record history file; and shall provide the capability for only authorized individuals to delete the record history file.
Access privilege specifications related to administration of metadata	**C2.2.1.1.** RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers. **C2.2.1.2.** RMAs shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data. **C2.2.1.3.** RMAs shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. **C2.2.1.5.** RMAs shall provide the capability to allow only an

	authorized user to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields. **C2.2.3.3.** RMAs shall provide the capability for only authorized individuals to create, edit, and delete record metadata components, and their associated selection lists. **C2.2.3.4.** RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization. **C2.2.3.7.** RMAs shall provide the capability for authorized individuals to arrange record metadata components and user defined record components on data entry screens to be used for filing. **C2.2.3.12.** RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g. project number, budget line) for site-specific requirements. **C2.2.3.21.** RMAs shall provide the capability for only authorized individuals to modify the metadata of stored records. However, RMAs shall not allow the editing of metadata fields that have been specifically identified in this Standard as not editable. **C4.1.12. <u>Editing Records</u>.** RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.
Access privilege specifications related to administration of records schedules	**C2.2.2.1.** RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories. RMAs shall provide the capability for defining multiple phases within a disposition schedule. **C2.2.2.2.** RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category: **C2.2.2.2.1.** Retention Period (e.g., fiscal year). **C2.2.2.2.2.** Disposition Action (interim transfer, accession, permanent, or destroy). **C2.2.2.2.3.** Interim Transfer or Accession Location (if applicable). **C2.2.2.5.** RMAs shall provide the capability for rescheduling

	dispositions of record folders and/or records during any phase of their life cycle if an authorized user changes the disposition instructions. This requirement includes the capability to change the cutoff interval of disposition instructions and to change the retention period associated with a disposition. **C2.2.3.15.** RMAs shall provide the capability for only authorized individuals to change a record folder or record category associated with a record. **C2.2.6.1.4.** RMAs shall provide authorized individuals with the capability to indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions. **C2.2.6.3.1.** RMAs shall be capable of implementing cutoff instructions for scheduled and unscheduled record folders. RMAs shall identify record folders eligible for cutoff, and present them only to the authorized individual for cutoff approval. The cutting off of a folder shall start the first phase of its life cycle controlled by the records schedule. **C2.2.6.4.1.** RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition. **C2.2.6.4.2.** RMAs shall identify record folders and/or records that have been frozen and provide authorized individuals with the capability to unfreeze them.
Access privilege specifications related to closing of record folders	**C2.2.6.2.1.** RMAs shall provide a capability for authorized users to close record folders to further filing after the specified event occurs. **C2.2.6.2.2.** RMAs shall provide the capability only to authorized individuals to add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing. **C2.2.6.3.2.** RMAs shall provide the capability to only authorized individuals to add records or make other alterations to record folders that have been cut off.
Access privilege specifications related to	**C2.2.5.3.** RMAs shall allow only authorized individuals to move or delete records from the repository.

retention, transfer, deletion, and destruction of records	**C2.2.6.5.4.** RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed. RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned. **C2.2.6.6.2.** RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed. **C2.2.6.6.4.** RMAs shall restrict the records destruction commands to authorized individuals.

Annex A

Table 4:
Detailed User-type Roles

Table 4, along with the introduction to it, is reproduced below directly from the DoD 5015.2 standard. It is included here to provide further details on how the standard differentiates between specific types of “authorized individuals.”

C2.2.7. Access Control. Table C2.2.7. summarizes requirements that refer to “authorized individuals” and offers additional information regarding example user-type roles and responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users. RMAs shall provide the capability to allow organizations to define roles and responsibilities to fit their records management operating procedures.

Table C2.2.7. Authorized User Requirements

Requirement	Application Administrator	Records Manager	Privileged User
C2.2.1.1. Create, edit, and delete file plan components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters file plan data	None
C2.2.1.2. Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.	Ensure database is correctly set up and installed	Define Lists	User abilities
C2.2.1.3. Create, edit, and delete record folder components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters folder data	Enters folder data
C2.2.1.5. Define and attach user-defined business rules and/or access logic to metadata fields including user-defined fields.	Creates rules and connects them to fields.	Manually execute rules if necessary	None

Table C2.2.7. Authorized User Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privilege d User**
C2.2.2.1. View, create, edit, and delete disposition schedule components of record categories.	Ensures that data structures are correctly installed and database links are in place	Enters disposition data, enters event data, closes folders.	Enters event data and closes folders.
C2.2.2.2. Define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category . . .	Ensures that data structure is correctly installed and database links are in place	Enters criteria and phase information	None
C2.2.2.5. Change the disposition instructions.	None	Edits disposition information and manually executes rules necessary to reschedule	None
C2.2.3.3. Create, edit, and delete record metadata components, and their associated selection lists.	Ensures that data structure is correctly installed and database links are in place	Creates Selection Lists	Enters data (all users)
C2.2.3.4. Select where data collection for optional metadata fields is mandatory for a given organization.	During Setup	Advising	None
C2.2.3.7. Arrange record metadata components and user defined record components on data entry screens to be used for filing.	During Setup	Advising	None
C2.2.3.12. Define and add user-defined metadata fields (e.g. project number, budget line) for site-specific requirements.	During Setup	Advising	None
C2.2.3.14. Limit the record folders and record categories presented to a user or workgroup.	Record Categories during setup	Record Folders	Record Folders
C2.2.3.15. Change a record folder or record category associated with a record.	As necessary	As necessary	None

Table C2.2.7. Authorized User Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
C2.2.3.16. Change or delete links and associations.	Database is correctly installed and configured	Change links as necessary	Make Links
C2.2.3.21. Modify the metadata of stored records.	As necessary	Change data as necessary	Time-Event and Event folders
C2.2.5.3. Move or delete records from the repository.	As necessary	As necessary	None
C2.2.6.1.4. Indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions.	Database setup	Link dispositions to record categories	Enter event information
C2.2.6.2.1. Close record folders to further filing after the specified event occurs.	As necessary	As necessary	As necessary
C2.2.6.2.2. Add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.	As necessary	As necessary	As necessary
C2.2.6.3.1. Approve cutoff.	As necessary	Routine work	None
C2.2.6.3.2. Add records or make other alterations to record folders that have been cut off.	Database support	Enters limits	None
C2.2.6.4.1. Extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.4.2. Unfreeze capability.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.5.4. Delete the records and/or related metadata after successful transfer has been confirmed.	As necessary	As necessary	None
C2.2.6.6.2. Confirm the delete command, before the destruction operation is executed.	As necessary	As necessary	None
C2.2.6.6.4. Access to records destruction commands.	As necessary	As necessary	None

Table C2.2.7. Authorized User Requirements

Requirement	Application Administrator	Records Manager	Privilege d User
C2.2.6.7.1. Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	Ensuring database structure is adequate and correctly installed	Enters cycling data	Cycles and Updates Records
C2.2.8.2. Determine which of the specified actions listed in C2.2.8.1. are audited.	Manage Audits	None	None
C2.2.8.3. Set up specialized reports to determine what level of access a user has, what records each user accessed, and what operations were performed on those records and associated metadata.	Create Reports	None	None
C2.2.8.6. Report audit information to authorized individuals.	Execute audit	None	None
C2.2.8.8. Backup and remove audit files from the system.	Backup and remove Files	None	None
C3.2.1. (Optional) Make global changes to the record categories, record category identifiers, disposition instructions, disposition instruction identifiers, and originating organization.	As necessary	As necessary	None
C3.2.2. (Optional) Bulk load capability.	As Necessary	As Necessary	None

InterPARES Project

International Research on Permanent Authentic Records in Electronic Systems

Appendix 14.3

Mapping of InterPARES Authenticity Task Force Benchmark Requirements for Version July 2001 against MoReq specification

Prepared for the Authenticity Task Force by
Maria Guercio
31 July 2001

Scope of MoReq

The specification describes Model Requirements for the Management of Electronic Record (MoReq). It is written to be “equally applicable to public and private sector organisations which wish to introduce an Electronic Records Management System (ERMS) or which wish to assess the ERMS capability they currently have in place”.

The Model focuses on functional requirements, even if it considers the relevance (but also the variety between environments of non-functional attributes (identified, but described only in outline).

The management (even electronic) of physical records, is partially addressed but not with reference to the detailed functionality associated with tracking physical locations, bar coding, etc.

The specification is designed as a practical tool and is intended to be used:

- by potential ERMS users as a basis for preparing an invitation to tender
- by ERMS users as a basis for auditing or checking an existing ERMS
- by training organisations as a reference document for preparing records management training and as course material
- by academic institutions as a teaching resource
- by ERMS suppliers and developers to guide product development by highlighting functionality required
- by record management service providers to guide the nature of the services to be provided
- by potential users of outsourced record management services as an aid in specifying the services to be procured.

The specification has taken into account the archival science and records management disciplines but it is designed for practical needs and for this reason it includes the incorporation of requirements for document management, workflow, metadata and other related technologies. It is intended to cover a wide range of requirements, for different countries, in different industries and different types of records.

The organisation of the specification

The specification is organised in chapters. Each chapter (specifically,, 3 to 11) contains a logical grouping of functional requirements: 3. classification scheme, 4. controls and security, 5. retention and disposal, 6. capturing records, 7 referencing, 8 searching, retrieval and rendering, 9. administrative functions, 10. other functionality, 11. non functional requirements. Chapter 12 identifies the metadata elements which are needed to meet these requirements, Chapter 13 contains a formal reference model.

The requirements includes at the same time benchmark requirements to guarantee the reliability of the ERMS and also requirements for improving its performance.

Table 1:
Detailed Mapping of InterPARES Requirements Against Provisions of MoReq Specification

INTERPARES BENCHMARK REQUIREMENTS	MOREQ REQUIREMENTS	
To support a presumption of authenticity the preserver must obtain evidence that: **REQUIREMENT A.1:** **Expression of Record Attributes and Linkage to Record** the value of the following attributes are explicitly expressed and inextricably linked to every record. These attributes can be distinguished into categories, the first concerning the identity of records, and the second concerning the integrity of records. **A.1.a:** identity of the record:		
A.1.a.i: Names of the persons concurring in the formation of the record (that is, the names of the author, writer, addressee, originator)	12.7.3. 12.7.6.	Author Addressee
A.1.a.ii: Name of action or matter	12.4.2. 12.4.3. 12.4.22. 12.7.2.	Name Descriptive keywords refs Keywords-based name Subject
A.1.a.iii: Date (that is, document, archival and transmission dates)	6.1.2. 6.1. 7.	Capturing the date of record creation Recording the date and time of registration as metadata

	12.7.5. Date/time 12.7.8. Registration date/time 12.7.22. Date sent 12.7.23. Date received
A.1.a.iv: Expression of archival bond (for example, classification code, file identifier)	3.1.1 to 3.1.9. Configuring the classification scheme in an ERMS able to represent files, with naming mechanism at configuration time for the capture or importation of electronic records 3.2.1. Metadata for files and classes in the classification scheme 3.2.2. Naming mechanisms for electronic files and classes in the classification scheme 3.2.4. Date of opening of a new class or file within the file's metadata 3.2.5. Inclusion in each new class or file metadata those attributes which derive from its position in the classification scheme) 3.2.10. Automatic creation and maintenance of a list (or repertory) of files 3.3.1 to 3.3.6. Managing the volumes, used to subdivide files too large 3.4.1 to 3.4.14. Maintaining the classification scheme with the specific aim of keeping a clear trace of classes, files, volumes or records in the case of reclassification 6.1.1. Capturing process able to provide controls and functionality to register and manage all electronic records regardless of the method of encoding and other technological characteristics 6.1.2. Taking into the ERMS the content of the electronic record, including information defining its form and rendition and information defining the structure and behaviour of the electronic record, retaining its structural integrity, information about the electronic document, the date of creation and other document metadata about the elements of the record, information about the context in which the record was originated, information about

		the application program, including its version
	6.1.3.	Capturing of all metadata elements specified at systems configuration and retain them with the electronic record in a tightly-bound relationship at all times
	7.1.1.	Associating to each class, file, volume, record a unique identifier to be stored as metadata elements of the entities to which they refer
	12.3.	Classification scheme metadata elements
	12.4.	Class and file metadata elements
	12.5.	Metadata elements for file or file volume
	12.6.	Volume metadata elements
	12.7.	Record metadata elements
	12.7.1.	Unique identifier
	12.7.24.	Links to related records
	12.7.13.	Preservation metadata
A.1.a.v: Indication of attachments		
A.1.b: integrity of the record:		
A.1.b.i: Name of handling office	12.3.1.	Name of the organisational unit responsible for the classification scheme
A.1.b.ii: Name of office of primary responsibility (if different from handling office)	12.4.7.	Person or post responsible for maintenance
A.1.b.iii: Indication of types of annotations added to the record	MoReq specification concerns annotations made in the course of handling the record itself for the purpose of managing it as part of the agency's records: classification code (3.2.1, 3.2.2, 3.2.4, 3.2.5), registration number, draft/version number, cross-references (3.4.1.1) to other record, etc.	

A.1.b.iv: Indication of technical modifications

REQUIREMENT A.2:
Access Privileges
the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records;

3.2.1. Restriction to Administrators of the ability to add to or amend classification scheme metadata after a records has been captured

3.4.5. Identification of the responsibility and reason for reclassification

3.4.7. Definition of a specific Administrator procedure for closing an electronic file

4.1.3. Definition of access roles as manager, clerk, analyst, database administrator

4.2.6. Capturing and storing in the audit trail information about date and time of capture of all electronic records, re-classification of record and file, change to the retention schedule, change to any metadata associated with classes, files, records, date and time of creation, amendment and deletion of metadata, changes made to the access privileges affecting file, record or user, export or transfer actions carried out on an electronic file, date and time of a rendition, deletion/destruction actions on an electronic file or record

4.5.1 Restricting access to system functions according to user's role to protect the authenticity of electronic records

4.5.2. Providing a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent authenticity (i.e. the absence of a valid and required electronic signature)

4.5.3. Providing a warning if an attempt is made to capture a record when the future verification of its authenticity is not possible

4.5.4. Preventing any change to the content of the electronic record by users and administrators

5.1.1. to 5.1.18. Providing functions for retention schedules (specification,

	reporting, destruction actions, integrated facilities for exporting records and metadata, association with classification scheme, tracking retention period, etc.) 5.2.1 to 5.2.11. Checking files which have reached the date or event specified by a retention schedule (by notifying them regularly to the administrator with the metadata information, alerting of other links, requiring confirmation for destruction, supporting reporting and analysis tools as lists, tracking in the audit trail all decisions taken) 5.3.1. to 5.3.17. Providing well managed process for transferring or exporting records and file, and for their destruction (inclusion of metadata, control of the integrity, exporting of all component of an electronic record as an integral unit, maintaining all links between records an metadata, between record, volumes and files) 12.4.8. User group access rights 12.4.9. User access rights 12.4.10. Security category 12.4.21 Other access information 12.7.9. User group access rights 12.7.10. User access rights 12.7.11. Security category
Requirement A.3: **Protective Procedures: Loss and Corruption of Records** the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records;	3.4.3. Restriction to Administrators of the ability to move classification scheme classes, file, volumes and records 3.4.4. Keeping a clear trace (at a minimum stored in the audit trail) of the reclassification of classes, files, volumes and records 3.4.6. Prevention of the deletion of an electronic file or any part of its contents at all time with the exceptions of destruction in accordance with a retention schedule (requirements 5) and

deletion by and Administrator as part of an audited procedure (requirement 9.3)

4.1.1. Administrator’s ability to limit access to records, files and metadata to specified users or user groups

4.1.2. Administrator’s ability to attach to the user profile attributes for user access (authentication mechanism like password)

4.1.10. Exclusion from the search result list of any record which the user does not have the right to access

4.1.11. Logging in the audit trail of any unauthorised attempts to access files, volumes or records

4.1.12. Capability of limiting user’s access to parts of the file repertory as specified at configuration time

4.2.1. Unalterable audit trail capable of automatically capturing and storing information about all the actions taken upon an electronic record, electronic file and classification scheme, the users and the date and time related to the event

4.2.2. Tracking events automatically within an audit trail procedure

4.2.3. Maintaining the audit trail for as long as required (at least for the life of the electronic record or file to which it refers)

4.2.4. Providing an audit trail of all changes made to group or individual electronic files, volumes, records, documents and related metadata

4.2.5. Providing an audit trail of all changes made to administrative parameters

4.2.6. Capturing and storing in the audit trail information about date and time of capture of all electronic records, re-classification of record and file, change to the retention schedule, change to any metadata associated with classes, files, records, date and time of creation, amendment and deletion of metadata, changes made to the access privileges affecting file, record or user, export or transfer actions carried out on an electronic file, date and time of a rendition, deletion/destruction actions on an electronic file or record

4.2.8. Making the audit trail available for inspection on request

4.2.9. Making the audit trail able to be exported for specified records, files or groups of file

4.2.10. Making the audit trail able to capture and store violations and attempted violations of access control mechanisms

4.2.11. Providing reports for actions on classes, files and records

4.3.1 to 4.3.7. Back up and recovery procedures, including the capability of selecting vital records

4.4.1 to 4.4.3 Tracking record movements

4.5.1. Restricting access to system functions according to user's role to protect the authenticity of electronic records

4.5.2. Providing a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent authenticity (i.e. the absence of a valid and required electronic signature)

4.5.3. Providing a warning if an attempt is made to capture a record when the future verification of its authenticity is not possible

4.5.4. Preventing any change to the content of the electronic record by users and administrators

4.6.1 to 4.6.12. If required for national security and other reasons, allowing the use of a scheme of security categories and security clearances

9.1.1. Providing recovery and rollback facilities in the case of system failure or update error

9.3. Requirements for changing, deleting and redacting records

REQUIREMENT A.4: **Protective Procedures: Media and Technology** the creator has established and implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change;	4.4.3.	Maintaining access to the electronic record content including the ability to render it and including maintenance of its structure and formatting over time and through generations of office application software
	5.3.14.	If records are stored on write-once media, providing facilities to prevent access to them so that they cannot be restored by normal use of the ERMS or by standard operating system utilities
	6.1.1.	Capturing process able to provide controls and functionality to register and manage all electronic records regardless of the method of encoding and other technological characteristics
	9.1.4.	Monitoring available storage space and notifying administrators when action is needed because available space is at a low level or because it needs other administrative attention
	9.1.5.	Monitoring error rates occurring on storage media and reporting to the Administrator
	11.7.1.	Control of the environment as compatible with storage media desired /expected life within the tolerance of the media manufacturer’s specification
	11.7.2.	Features for the automated periodic comparison of copies of information and the replacement of any copy found to be faulty to guard against media degradation
	11.7.3.	Capability of allowing the bulk conversion of records to other media and/or systems in line with the standards relevant for the format(s) in use
	11.7.4.	Adopting a programme for upgrades to the ERMS technology base that allows for the existing information to continue to be accessed without changes to the content
	11.7.5.	Using widely-accepted standard which are the subject of open and publicly available specifications for encoding, storage and database structures

	11.7.6. Fully documenting any proprietary encoding or storage or database structures 11.7.7. Managing a range of preservation metadata elements for the records and their component parts (see 12.7.13)
REQUIREMENT A.5: **Establishment of Documentary Forms** the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator;	6.3.1. to 6.3.6. Capability of capturing documents from a range of different electronic document format types and structures as records, specifically the most commonly used office documents 12.7.7. Record type
REQUIREMENT A.6: **Authentication of Records** if authentication is required by the juridical system or the needs of the organization, the creator has established specific rules regarding which records must be authenticated, by whom, and the means of authentication;	4.5.2. Providing a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent authenticity (i.e. the absence of a valid and required electronic signature 10.5. Capability of retaining the information of electronic signature in their different technologies and checking its validity 10.6. Capability of applying encryption mechanism 10.7. Capability of applying watermarks mechanism 12.7.20. Electronic signature 12.7.21. Electronic signature 12.7.28. Authentications 12.7.29. Encryption information, watermark information
REQUIREMENT A.7: **Identification of Authoritative Record** if multiple copies of the same record	12.8.2. Identifier of original record

exist, the creator has established procedures that identify which record is authoritative;	
REQUIREMENT A.8: **Removal and Transfer of Relevant Documentation** if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator has established and implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records.	5.3.2. Inclusion of metadata associated to any class, file or volume to be transferred 5.3.4. Inclusion of a copy of all the audit trail data associated with the records, volumes and files being transferred 5.3.5. Providing a utility or conversion tool to support the rendition of records marked for transfer into some approved transfer formats(s) 5.3.6. Producing a report detailing any failure during a transfer, export or deletion (it must identify any record destined for transfer, which have generated processing errors and any files or records which are not successfully transferred, exported or deleted 5.3.12. Providing the ability to generate user-defined forms to describe electronic files that are being exported or transferred 9.2. contains reporting requirements not specifically related to the preservation aims: reports on audit trail, report listing of files and volumes according to the classification scheme. 12.4.17. Retention schedule 12.5.1. Retention schedule 12.7.13. Preservation metadata

Many elements in the requirements for metadata (see)