TLA Standards Digital Learning Acquisition Guidance

August 2022

Advanced Distributed Learning

Distribution A. Approved for public release: distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
1-08-2022	Document and Reference Guide	07/10/2021 - 30/07/2022

4. TITLE AND SUBTITLE
TLA Standards Digital Learning Acquisition Guidance

5a. CONTRACT NUMBER
FA701420D007

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
0603769D8Z

6. AUTHOR(S)
Mr. Andy Johnson and Mr. Shawn Miller

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
FA701421F0184

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
OUSD Personnel & Readiness
Advanced Distributed Learning Initiative
13501 Ingenuity Drive, Suite 248
Orlando, Florida 32826

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
OUSD Personnel & Readiness
Advanced Distributed Learning Initiative
13501 Ingenuity Drive, Suite 248
Orlando, Florida 32826

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD/P&R/DSSC/ADLI

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The founding goal of using standards within acquisition of distributed learning content and technology is to reduce cost in both current and future acquisitions and collaborative efforts across organizations. This document explores existing successful acquisitions and supplies that language as well as successful ways to implement best practices of standards and to identify mature standards (as a part of the ADL research portfolio, the Total Learning Architecture (TLA)). It provides a reference both by technical standard, the standards associated technology, and the standards associated use cases as tied to that technology. This document is intended to updated periodically.

15. SUBJECT TERMS
Total Learning Architecture, Standards, TLA, Acquisition, Acquisition Language, cmi5, xAPI, Experience API, Test Suite, Conformance, Conformance Testing, Content, Content Testing, Package, LMS, SCORM Replacement, standards, AICC, SCORM, xAPI Profile, interoperability, metadata, competencies, P2881, Shareable Competency Definition, SCD, IEEE, 1484.20.3

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
U	U	U	UU	49	Sae Schatz
					19b. TELEPHONE NUMBER *(Include area code)*
					571-480-4640

TLA Standards Digital Learning Acquisition Guidance

Andy Johnson, ADL Initiative (SETA)
Shawn Miller, Defense Acquisition University

August 2022

Table of Contents

1.0 Executive Summary

The purpose of this document is to provide guidance to assist Department of Defense (DoD) acquisition personnel on integrating learning technology standards into their acquisition processes. It works in concert with the Department of Defense Instruction (DoDI) 1322.26 as documentation on how to reach requirements within that instruction and within the updated reference.

The current version of this document has overarching recommendations for how to implement the Total Learning Architecture (TLA), which is seen as the means by which to achieve DoD Learning Modernization. The TLA focuses on technical specifications and standards as those means.

This document focuses on implementation of three standards within the TLA. The first standard is the Experience Application Programming Interface (xAPI), which is a standard for tracking learner performance. The second standard is cmi5, which is structured xAPI data for the Learning Management System/content session and registration use case. Finally, the Institute of Electrical and Electronics Engineers (IEEE) P2881 Standard for Learning Metadata allows for search, discovery, and curation of learning content by applying attributes to learning objects. All digital learning content can be considered learning objects, whether they are graphics in a repository, a distributable lesson that is integrated into training, or a course offering with a specific course instructor or a specific session slot of a simulator.

This document is expected to be transitioned to a more suitable web format as opportunities arise and will be updated approximately once each year.

2.0 INTRODUCTION

The TLA is a research and development project sponsored by the ADL Initiative and conducted in collaboration with stakeholders from across the defense community, professional standards organizations, industry, and academia. It includes a set of technical specifications, standards, and policy guidance that define a uniform approach for integrating current and emerging learning technologies into a learning services environment. Within this environment, multiple services and learning opportunities (of various modalities and points of delivery) can be managed in an integrated, interoperable 'plug and play' environment.

The Department of Defense Instruction (DoDI 1322.26) and its references define the most current technical requirements and best practices for distributed learning across the DoD and is one of the key policies of the TLA. DoD Components are encouraged to refer to these references on a regular basis. While the DoDI 1322.26 doesn’t explicitly discuss TLA compliance, compliance to TLA standards is referenced in the Instruction by listing standards that are mandated unless exceptions are provided, including xAPI and cmi5. While the P2881 Learning Metadata standard is not listed as mandated, it is anticipated that it will be in the near future and has guidance to prepare DoD as such. This document is intended to align to the DoDI 1322.26 requirements. Some DoDI requirements will be repeated in this document. This doesn’t mean they are any more or less important to the overall compliance of the DoDI. Acquisition guidance should always consider the information in the DoDI 1332.26.

IEEE 9274.1.1 or xAPI are both a learning technology standard and a suite of web-service application programming interfaces (API) that support a simple object-based model for describing, recording, and sharing individual or team performance across digital learning systems. The xAPI specification requires the use of a Learning Record Store (LRS), which is the server-side implementation of xAPI. The LRS allows xAPI data to be shared with other systems that require access to these data. Additional information and access to the standard is available on the ADL Initiative’s GitHub site (https://github.com/adlnet/xAPI-Spec/blob/master/xAPI-About.md#partone).

cmi5 is a specification that includes an xAPI Profile and allows all the functionality of Sharable Content Object Reference Model (SCORM®) with the benefits of xAPI. The cmi5 specification replicates SCORM functionality, with the intention of replacing SCORM as the de-facto format of online courses and traditional computer-based training. Products that fully support cmi5 will also support xAPI. Additional information and resources are available at the cmi5 Project on GitHub (https://aicc.github.io/CMI-5_Spec_Current/)

The P2881 Learning Metadata Standard was created to align to modern distributed learning practices. While psychological and pedagogy practices are very slow to change, new technologies enable new possibilities such as Augmented Reality (AR) and Virtual Reality (VR). Content publication practices have evolved to fit the expanding modalities of mobile and beyond. The notion of a content repository has changed to be more of a cloud-based, distributed solution. Ideas for how metadata can be created, and the management of those vocabularies has changed accordingly to the digital and away from the physical, away from being designed for human consumption and toward machine consumption. This standard specifies a conceptual data model that defines the structure of a metadata instance. This conceptual data model specifies the data elements which compose a metadata instance for any type of Learning Object.

2.1 How To Use This Document

This document introduces a general TLA compliance strategy in Section 3. That section describes compliance and outlines how the later sections can be used to achieve TLA compliance. Section 3 should be considered a longer-term roadmap on how to perform acquisition on a holistic TLA solution but is currently limited in scope. Each of the next sections, in the case of this document, Sections 4-6, each describe a standard necessary for TLA compliance and the details on how to successfully perform acquisition of that standard. Section 4 will describe how to implement xAPI, Section 5 will describe how to implement cmi5, and Section 6 will describe how to implement P2881 Learning Metadata. The structure for each section provides use case narratives that each contain acquisition language and possible criteria/metrics for evaluation. Related documentation, best practices, pitfalls to avoid, and cybersecurity concerns are provided for each standard (as opposed to being specific to the use case). Each of Sections 4-6 can be used as a starting point to implement the specific standard referenced by that section. As cmi5 is derived from xAPI, it refers to the xAPI Section often rather than simply copy/pasting the same requirements.

This document makes use of real acquisition language. In describing the text as “real”, it means it was used in the Statement of Work/Performance Work Statement of a successful DoD contract. That language is shown in quotes and is introduced by supplemental text. Quoted text that is not from a contract will be cited (most often the DoDI 1322.26). Modifications to this text will appear in ***bold italics*** and will be used only if the original language was insufficient or inaccurate. Other suggestions will appear in best practices for such sections. The amount of real language will increase over time. Sections that do not have quoted example language have not been used but have been carefully considered by standards experts and by those with acquisition experience.

This document uses specific requirements-based language to indicate the level of adherence to be compliant. The terms “shall” and “must” refer to unconditional adherence (this document recommends “shall” but recognizes that existing language sometimes uses “must”). Conversely, “shall not” and “must not” indicate adherence against certain conditions (for functional purposes, “may not” is the same as “shall not” and “must not”). The terms “should” and “should not” indicate best practices in favor of or not in favor of a condition. Some requirements list exceptions to rules and times where not following the typical best practice may itself be a best practice. Any instances of the word “may” indicate that the specific condition was considered and found to be acceptable. Lack of a “may” condition doesn’t mean that it is not allowed (e.g., an implementation detail not covered at all in this document). There may be DoD policies that change or organizational processes that override requirements and recommendations in this document. In those cases, DoD/Organizational policies shall be followed. This does not necessarily mean that such an implementation is not aligned to the standard in the section where such a conflict occurs.

2.2 Glossary

The following terms are useful to know as background to TLA compliance:

Assignable Unit (AU): A learning content presentation launched from an LMS. The AU is the unit of tracking and management. The AU collects data on the learner and sends it to the LMS.

cmi5 – cmi5 is a “profile” for using the xAPI specification with traditional learning management (LMS) systems. The cmi5 profile ensures plug and play interoperability between learning content and LMS systems. The use case that the cmi5 profile is specifically designed for is one where a user launches a content/activity from the LMS user interface.

Competency – Short for competency definition. A competency is the set of skills and behaviors required in the performance of a task or activity within a specific context. The competency definition is a resource that includes a statement that describes a competency and may include a specific context and reference definitions of potential levels of proficiency. For simplicity's sake, this document uses just a single definition and considers competencies to be of varying granularity.

Competency Framework – A resource that identifies a collection of logically related competencies and how they are associated, related, and contextualized. A Competency Framework is often under ownership by a DoD Component and therefore takes on the context of that DoD Component.

Course –- A collection of assignable units, in a logical grouping, of learning content. A course is typically an internal data structure. Courses are often assigned to learners and tracked by the LMS. A course can be represented by an external format and/or allocate all resources or links to resources in a course package.

Experience Application Programming Interface/Experience API (xAPI) - The collection of rules articulated in the xAPI standard (https://opensource.ieee.org/xapi/xapi-base-standard-documentation/-/tree/main) which determines how learning experiences are defined, formatted, and exchanged so that independent software programs can exchange and make use of this information.

Internationalized Resource Identifier (IRI) - A unique identifier which could be an IRL (same relationship a URL has with a URI). Used to identify an object such as a verb, activity, or activity type. Unlike URIs, IRIs can contain some characters outside of the ASCII character set to support international languages. IRIs always include a scheme. This is not a requirement of these standards, but part of the definition of IRIs, per RFC 3987.

Learning Management System (LMS) – A set of web services that authenticates a learner, authorizes them to take certain distributed learning content, and tracks progress within that content. Many acquisitions use/used an LMS that functioned less as a series of services and rather as a single software solution.

Learning Record - An account of a learning experience that is formatted according to the rules of xAPI. A Learning Record takes on many forms, including Statements, documents, and their parts. This definition is intended to be all-inclusive.

Learning Record Provider (LRP) - An xAPI Client (any entity that might interact through requests) that sends data to Learning Record Store(s). Often, the Learning Record Provider creates Learning Records while monitoring a learner as a part of a Learning Experience.

Learning Record Store (LRS) - A server (i.e., system capable of receiving and processing web requests) that is responsible for receiving, storing, and providing access to Learning Records.

Learning Object - Defined as any entity, digital or non-digital, that is used for learning, education, or training. A Learning Object in the P2881 standard is the generic classification of one of three scopes: Asset, Learning Resource, and Instantiation.

Learning Tools Interoperability (LTI): A standard from IMS Global that allows the connection and sharing of data across learning applications securely. This standard is in wide use within Learning Management Systems and their connected applications.

Shareable Content Object Reference Model (SCORM) – A standard that was made up of a set up standards that provided a baseline of functionality to distributed learning systems. This legacy approach paired a single learner with a single course while being tracked by a Learning Management System.

Statement - A data structure showing evidence for any sort of experience or event which is to be tracked in xAPI as a Learning Record. A set of several Statements, each representing an event in time, might be used to track complete details about a learning experience.

Total Learning Architecture (TLA) - The Total Learning Architecture is a research and development project sponsored by the Advanced Distributed Learning (ADL) Initiative that consists of a set of internet and software specifications being developed to create the interoperability backbone of the future learning environment enabled by DoD modernization.

xAPI [Application] Profile: A specific set of rules and documentation for implementing xAPI in a particular context. A profile provides a way to talk about vocabulary concepts, statement templates, and patterns for xAPI data.

Universally Unique Identifier: A unique label (globally unique, not just to the local installation) applied to information in a computer system. For the purpose of this document, it is synonymous with a globally unique identifier (guid).

2.3 Acquisition Roles and Responsibilities

This document will define only a minimal number of roles. Responsibilities will be addressed in the context of the specific acquisition language for each standard in Sections 4-6.

DoD Component – an organization that is acquiring TLA-compliant technology, implementing TLA standards, and is the controller of their organizational environment. “DoD Component” is substituted for the actual organization in the sample language.

DoD Component Team – agents of a DoD Component that perform actions, ideally in compliance with this document.

Contractors/Vendors – agents that produce technology or services for a DoD Component but are not part of the DoD Component Team.

This document is agnostic to whether DoD Component Teams or Contractors/Vendors are used. When this document refers to Contractors or Vendors, it is considered to be done at the direction of a DoD Component Team. Any responsibility of a DoD Component Team may be offloaded, at the DoD Component’s discretion, to a Contractor or Vendor.

3.0 TLA COMPLIANCE

The following section describes the current state of TLA compliance. As future versions of this report are released, this section will be updated accordingly. Currently, the focus is only on specifications and standards. For future cycles, the Capability Maturity Models referenced in the TLA Quick Start Guide may be incorporated.

3.1 What is TLA Compliance?

TLA compliance is defined as strict adherence to TLA standards. This adherence should be measured by conformance testing whenever possible. Conformance testing software creates functional tests that directly correspond to documented requirements that exist in standards. Conformance tests cannot test all requirements in standards, but TLA standards are written such that all "SHALL" requirements are testable by software. Not every TLA standard currently has a conformance test. The most effective means of achieving compliance to that standard is through mutual agreement between the producers and consumers of the data from that standard.

3.2 Current Compliance Procedures

TLA compliance is very loosely defined at this time. TLA Compliance is considered to be compliance to each of the separate standards referenced in Sections 4-6. At this time, no software, systems, or processes are considered that connect TLA standards or implementations. To summarize the external software validation requirements, the current procedure dictates that all LRSs are validated by the ADL Conformance Test Suite (https://lrstest.adlnet.gov/), and that all cmi5 LMSs and content is validated by the cmi5 Conformance Test Suite and Player (https://github.com/catapult-project/catapult). At this time self-installation is needed for the cmi5 tools. However, ADL Initiative may host a version in the future. Currently, only self-reporting is available as there are no 3rd party certification programs.

3.3 Overall Distributed Learning Requirements and Best Practices

The following requirements transcend all the TLA standards in this document:

- The DoD Component Team should undertake project planning and implementation activities covering development of data strategy, instrumentation of data, testing, training and operations and maintenance.
- The DoD Component Team shall provide adequate training on all acquisition to personnel that use them.
- The DoD Component Team shall leverage both coupling and authentication capabilities in a manner that offers user authorization to create and share data as appropriate.
- The DoD Component Team shall take appropriate measures shall be taken to maximize data integrity.
- The DoD Component Team shall require evidence of conformance test claims as supplied by Vendors and Contractors.
- DoD Components shall follow policy on distributed learning, data, and information technology, particularly DoDI1322.26 and DoDI8320.02.

4.0 xAPI Implementation

This section describes acquisition strategy for creation of an environment, also described as set of organizational web services that are linked together via data and are in compliance with the xAPI specification/IEEE 9274.1.1 standard. There are many web services that are oriented in different software packages (such as a Learning Management System) that can become xAPI compliant. These can be referred to as Learning Record Providers (LRPs) and LRSs. There are also systems that benefit from using the LRS, such as those using the data for analytics and visualizations. For the most part, learning content or authoring tools that produce learning content can be considered LRPs but without any of the communication requirements. In other words, the content should produce xAPI data that can simply be "bounced" by the LRP to the LRS without having to do any reconstruction/revalidation.

Conformance testing for LRSs is available via the xAPI Conformance Test Suite. LRPs are effectively tested by their communication with an LRS and that communication not returning errors. Vendors may self-report their successes at The ADL xAPI Adoption Website . In addition, xAPI Profiles are very important to creating interoperable data and should be used whenever possible. It is recommended that conformant profiles are used whenever possible from https://profiles.adlnet.gov/. More guidance and data conformance testing surrounding xAPI Profiles will be available in the future.

While keeping track of version support of xAPI is important, the xAPI Accreditation Report indicates that there are very few impacts of the migration from 1.0.3 to 2.0 on xAPI Adopters. The legacy browser support is one difficult issue, but the support of legacy systems as a whole is being driven out more by mobile technology and Operating System support. The new use of contextGroups and contextAgents is a small but necessary addition for LRSs to support. LRS Vendors indicated in an IEEE survey that they welcomed all the changes and that they bring more stability than additional work.

4.1 Use Cases

The use cases in this document are organized to be simplistic and categorical, such that they can be building blocks for creating high quality acquisition language. In this way, a set of use cases can be used to match as closely as possible to an organization's requirements. Subsets of use cases will be listed under each use case section.

Each use case in a subset will contain several format or domain specific high-level requirements that can be met, often using xAPI Profiles. This document will make general recommendations for the use of xAPI Profiles and will provide either generic links to the xAPI Profile Server such that the profile can be searched for or, when applicable, a specific xAPI Profile will be linked.

Sample acquisition language will be given in each of these sections and will be structured with the purpose of the language and then the quoted language.

4.1.1 Use Case #1 - LRS Integrated with Current Systems

While it is possible to acquire an LRS for standalone purposes, due to eventual capabilities not yet being acquired, this use case focuses on aligning and configuring all systems and services in a current environment to the newly acquired LRS.

Applications that can be integrated include but are not limited to:

- AR/VR Support
- Video Tracking
- Course Support (LMS)
- Specific Software Integration (e.g., Alexa, Teams)

Learning Tools Interoperability (LTI) https://www.imsglobal.org/activity/learning-tools-interoperability is a common standard that many LMSs adopt that allow the sharing of authenticated user information and system information across services. xAPI can leverage this integration if it exists within the organizational environment. Value added of implementing LTI from scratch for the purposes of xAPI has not been calculated as a part of this guidance.

4.1.1.1 Use Case #1 - Sample Acquisition Language

- The LRS shall support authentication using the DoD's Identity, Credentialing, and Access Management (ICAM) (https://dodcio.defense.gov/Library) policies.
- To establish the universal nature of the LRS, consider the following: "The LRS must be able to receive different events and activity streams via xAPI to include formal and informal learning, as well as the ability for users to self-report activities."
- To establish the diversity of integration expected, consider the following: "The LRS must be capable of integrating and receiving data from multiple systems within the Defense Acquisition University learning architecture and provide real-time tracking and recording of activity streams from multiple sources, including but not limited to:

    - Informal Learning Activities
    - Formal Learning Activities
    - Real-world activities
    - Games and Simulations
    - Mobile access
    - Team-based participation
    - Mentoring
    - AR/VR"

- To accurately define integration, consider the following: "Each system that becomes an LRP must be capable of sending statements with actor fields that correspond to an authenticated user on that system. For example, a course delivered via LMS would send data about the learner taking the course. Each system must send a statement with structure specified by DoD Component. Practices for adding additional statement types must be well documented."
- To effectively connect xAPI data to authenticated and authorized learners, consider the following: "It is recommended that LTI is used whenever practical to provide the user information to populate statements with the actor property."
- To effectively offload LRS support to a Contractor, consider the following "provide hosting, professional services, training, maintenance & technical support for a cloud hosted PaaS or SaaS LRS solution. "
- To provide onboarding service requirements for the LRS solution, consider the following: "The Contractor shall conduct all activities required to install and configure the LRS. Installation and configuration tasks are comprised of all activities including but not limited to:
    - Standing up all environments
    - Configuring initial system level settings
    - Establishing administrator user accounts
    - Establishing base system roles and permissions
    - Configuring management settings
    - Configuring initial authentication settings
    - Enabling out-of-the-box publishing standard capabilities
    - Configuring analytics settings, canned reports, custom reports, dashboards, and custom data visualizations."

- To create reassurances via demonstration, consider the following: “The Contractor shall deliver a comprehensive demonstration to the DoD Component product owner and systems administrators of the delivered LRS environments using Microsoft Teams or Zoom by the suspense date as indicated in section 11. The Contractor must cover in their product demonstration, all features and functionality within the LRS environments.”
- To provide effective classification of services for the LRS integration, consider the following: “The integration involves establishing the LRS application within the environment and suite of DoD Component applications. The Contractor shall provide Professional Services sufficient to deploy the LRS application and apply the approved LRS system configuration, establish interfaces and conduct testing based on the technical decisions made during the installation and configuration. The integration steps must cover both system and data levels for: unit testing, smoke testing
(build verification testing), integration testing and system testing performed by the Contractor with DAU personnel support. The approach, and execution timelines shall be incorporated into overall project planning activities.”
- To provide effective initial training of the LRS (e.g., including real-time support), consider the language below. This language can be used as a template for any such training that would accompany acquisition. “Contractor shall conduct comprehensive LRS onboarding training pertaining to administration and development activities within the LRS solution, and any integration points. The Contractor shall provide all required course materials, reference guides, job aides, developer docs, and community help resources. Training shall be conducted virtually using the Contractor’s preferred virtual meeting/training platform, recorded, and made available for later viewing.”
- To provide effective training materials of the LRS, consider the language below. This language can be used as a template for any such training that would accompany acquisition. “The Contractor shall provide comprehensive LRS training materials for tasks related to system administration, operations, and maintenance. Training materials shall be in any of the following formats: online course modules, videos, reference guides, and help articles, and made available to appropriately scoped user roles for asynchronous self-paced learning.”
- To provide effective technical support LRS, consider the language below. This language can be used as a template for any such support that would accompany acquisition of a software system. “The Contractor shall provide support services for the LRS solution, including self-service options, live technical support, and escalation through tier-3 engineering/system development services. Technical support is required to be provided through several channels including but not limited to a Contractor-hosted service management or ticketing system, email, an online support page that connects to FAQs, best practices, tutorials, and telephone. Contractor-provided service level agreements (SLAs) required to support timely issue handling and communication procedures as well as identify and address issues that must be handled immediately.”
    - To effectively establish the SLAs, consider the following language: The Contractor shall provide a standardized SLA covering all managed products and services. All Contractor technical support and maintenance work shall be performed in accordance with established SLAs. The Contractor must provide SLA terms including but not limited to:
        - The Contractor shall provide system availability 24x7x365 with uptime of no less than 99.9%

    - The Contractor shall provide service continuity, disaster recovery and backup operations, including hot and warm failover contingencies as well as documentation of remediation approaches
    - The Contractor shall provide data ownership policy, rights, and procedures for requesting deletion of Government and visitor data
    - The Contractor shall provide issue, ticket, request procedure thresholds and projected resolution times originating at each identified support service Tier
    - The Contractor shall provide software release management practices, including testing procedures, and advance notification periods allowing appropriate customer planning and communication for major, minor, and patch releases
- To establish a clear communication structure for requirements/issues, consider an issue matrix as Government Furnished Information and the following language: “The DoD Component will develop and share a backlog of open issues while system administrators work with the Contractor’s enablement team to install, configure, and implement the LRS solution. This log will be used as the primary tracking mechanism for all issues, action items, and decision points between the DoD Component and the Contractor prior to system implementation. Both parties shall communicate status updates through this log to ensure information tracked and open items are resolved in a timely manner.”
- Additional “a la carte” requirements can be found in the following matrix. (Note that these are possible useful requirements and are not specific endorsements of particular processes over another. All requirements were directly used in a successful LRS acquisition.)

Accessibility Requirements

- The LRS user interface must be compliant with Section 508 of the Rehabilitation Act of 1973 Public Law 106-246.
- The LRS user interface must be compliant with Rehabilitation Act Amendments of 1998 (29 U.S.C. 794(d))
- Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR Part 1194)
- The LRS user interface must be compliant with the Web Content Accessibility Guidelines (WCAG) 2.0.

Administrator UI/UX/Functional Requirements

- Authorized administrators must be able to configure the LRS user interface / Dashboard and reports to conform to the organization's design standards including:
    - Logo
    - Backgrounds (images, gradients)
    - Style sheets (fonts, colors)
    - Feature, control, and data labels
    - Instructions and prompts
- Authorized administrators must be able to configure client-defined security roles (e.g., Need to be able to configure for users, admin levels etc.).
- Authorized administrators must be able to control the read, write, execute, and delete permissions related to LRS functionality at a granular level for each security role.
- Authorized administrators must be able to assign/unassign security roles to users.
- The LRS must provide a report of user login dates and times and user logout dates and times, which:
- Includes, at a minimum, the user's first and last names, user ID, organization, and role.
- The LRS must provide a report listing all user accounts that have access to LRS system.

LRS Functional Requirements To Ensure "Good" Data

- Import and export of learner and course tracking data using standardized data interchange formats (e.g., XML, JSON, CSV) without writing high-LOE integration applications.
- The LRS must support xAPI Profiles to include: [named] profiles within all search, retrieval, visualization and analytics capabilities. This includes custom searched reports, menus, filters and data integrity for those Profiles.
- Ensure data integrity of statements generated by integrated systems and sent to LRS such that the LRS data is directly attributable from one of those systems and could not come from an outside source

Clarifications to Expected Behavior of an LRS
(Many of these are directly in the xAPI Standard, but are helpful to repeat)

- The LRS must comply with current ADL xAPI LRS Conformance Requirements and xAPI 2.0.
- The LRS must be able to receive xAPI data from user interactions originating from activity providers input
- The LRS must accept xAPI statements defined within xAPI Profiles
- (E.g., cmi5, video)
- The LRS must expose its endpoint to third party xAPI activity providers.
- The LRS must make its xAPI data fully accessible to third party analytics and reporting tools.
- The LRS must provide a method to display xAPI activities stored through reporting, queryable data, statement viewer and analytics dashboards.
- LRS must maintain a persistent storage of learning activity records (i.e., xAPI statements).
- LRS must capture all xAPI statements generated from Learning Record Providers (e.., Learning Activities)
- LRS must ensure that xAPI statements are conformant.
- LRS must provide a mechanism for administrators to purge xAPI records
- LRS must maintain a record of purges to show that data has been altered
- LRS must provide a mechanism to ensure the integrity of xAPI data stored
- LRS must be able to identify if an incoming xAPI statement is not well formed
- LRS must allow storage of xAPI statements for each UUID stored as actor
- LRS must be able to identify that an incoming xAPI statement is not from a registered device
- LRS must be able to identify incoming xAPI statement with an actor that is not a valid user, registered component, or identity group.
- The LRS must have a quality assurance process whereby changes to the xAPI spec or the LRS product are regression tested with an internal test suite to ensure strict compliance with the spec.
- LRS serves as endpoint and interfaces with systems of work within DoD Component's enterprise architecture through APIs

Data Viewing/Visualization Requirements

- The LRS must provide roles-based configurable dashboard views of user data and the ability to associate data with profiles and then users to profiles as well (e.g., a learner dashboard pulls in cmi5 data which is (verblist))
- The LRS must provide granular drill down to actual statements (with filters/ search by Activity ID, Verb ID, Agent Value, Agent Property, Context Category, Context Agent all found in xAPI 2.0).
- The LRS must provide a statement viewer function allowing filtering by organization hierarchy or multiple filters to customize defined groups.
- The LRS must provide out-of-the-box, predefined and customizable reports, and wide range of visualizations of data.
- The LRS must provide permission levels with different kinds of access to dashboards and reports.
- The LRS must provide enhanced query capability beyond the basic xAPI specification requirements by providing the ability to link and/or import data from alternative data sources.
- The LRS must provide flexible, robust abilities to create custom reports, both internally and by using external tools.
- The LRS must provide capabilities to:

    - browse xAPI statement data
    - use canned reports for commonly required data such as test scores
    - measure business impact (through integration with external BI systems such as Qlik)
- The LRS must provide analytics that include graph charting and advanced visualization options like video and multimedia engagement, heat mapping etc.
- The LRS must provide an ad hoc query report capability that enables an authorized administrator to select from a list of data categories.
- The LRS must provide authorized administrators to specify a list of report recipients for a given report and schedule automatic one-time or recurring delivery of the report to the recipient list via email.
- The LRS must provide configurable field level restrictions to be placed on all reportable fields, assignable through security role permissions.
- The LRS reporting tool must be user-friendly to the point that ad-hoc reports can be created and run with a minimum of user training.
- LRS must allow use of filters on retrieving xAPI data by Actor, date/time, activity type (object), verb, user specified extension field values

Data Viewing/Visualization Requirements

- The LRS must keep a log of all changes made to the LRS configuration and settings, who made them, and when made.
- The LRS should keep a log of all user accounts that have access to the LRS system and their actions for auditing purposes.
- LRS should send notifications based upon requirements in this category

System Security/Cybersecurity Requirements

- The LRS like other systems in our environment must be capable of supporting DoD Component's identity management solution using SAML 2.0 and integrate with DoD Component's Single Sign-On (SSO) solution, Oauth, WS Federation and OKTA.
- The LRS must be able to support Vanity URL/ Bring your own domain (e.g. (LRS.MYORG.MIL)
- LRS must include login credentials utilizing FIPS 140.2 encryption of passwords
- LRS must support the use of FIPS 140-2 encryption
- The LRS must provide Data at Rest encryption for data stored.
- The LRS must provide encryption of web services (i.e., REST, SOAP).
- The LRS must provide SSL encryption (HTTPS) for all web traffic.
- The LRS must provide a solution that enables manual and scheduled batch data management through flat files for routine system administration tasks including but not limited to user and content import/export, object synchronization, list cleanup, and removal of duplicative data across a variety of system data sources. Scheduled flat file import/export must be secured via SFTP or secure shell (SSH) using public key cryptography.
- LRS must allow for connections using REST over TLS
- The LRS must be able to pass minimum FedRAMP Impact Level 2 for public-facing cloud solutions and up to IL4 for protection of personally identifiable information when appropriate. For details, see: https://www.fedramp.gov/
- Allows configuration for the management of Personal Identifiable Information (PII) in accordance with enterprise and government policy (such as FERPA).
- Contains multiple security access levels with ready access to unclassified learning material and more stringent security requirements for Controlled Unclassified Information (CUI).
- The LRS must support compliance with Security Technical Implementation Guide (STIG), especially regarding system installation, maintenance, configuration management and administrative processes. For details, see: https://public.cyber.mil/dccs/.

- The LRS must support compliance with the Federal Information Security Management Act (FISMA), especially regarding information security controls, risk assessment, and monitoring. For details, see: [https://www.cisa.gov/federal-information-security- modernization-act](https://www.cisa.gov/federal-information-security-modernization-act)
- The LRS must be able to pass the DoD Risk Management Framework (RMF). For details see: https://csrc.nist.gov/projects/risk-management/rmf- overview.
- Level of FedRAMP authorization. The product must be capable of being hosted as a Platform as a Service (PaaS) or cloud Software as a Service (SaaS) or on- premises at the DoD Component and/or third-party hosting with applicable Federal and DoD certifications and authorizations (e.g., FedRAMP, FISMA, RMF). If not FedRAMP, willingness to obtain certification and authorization with DoD Component as a sponsor.

Hosting Requirements

- The LRS must be installed in multiple server environments including:
  - Test: for testing and acceptance, LRS updates, and systems integrations.
  - Production: for access by end users.
  - Continuity of Operations: mirrors production environment for failover and disaster recovery.
- The LRS vendor must inform the client of LRS system updates (major and dot releases, updates, and patches) at least 30 days in advance of the intended release date. As well, inform DoD Component if any of these updates impact any of the integrations/data from other systems (e.g., any API modifications).
- The LRS vendor must install a production-ready release of all LRS system updates (major and dot releases, updates, and patches) in a staging environment and provide up to 30 days after the release date for the client to test systems integrations. Once accepted by the client, the release must be installed in production during off-peak hours on a date and time agreed in advance to by the client.
- If not hosted, an on-premise solution must be load balanced across multiple servers.

Documentation Requirements

- The LRS vendor must provide documentation to demonstrate its quality process maturity, especially in relation to product enhancement, known bug prioritization and communications, and pre-release testing.
- The LRS vendor must provide documentation to demonstrate its release management process maturity with its product's release cycle history and future roadmap including the schedule, frequency and purpose of patches, dot releases and major releases.
- The LRS vendor must provide documentation to demonstrate its support process maturity with its support capabilities, structure, availability, scope, service levels, policies, and active user group forum/s with ongoing discussions.
- The LRS vendor must provide documentation to include training services, materials, and resources to support the LRS administrators and pilot users.
- The LRS vendor must provide documentation to demonstrate its privacy policy and practices including, but not limited to, a description of how LRS data is stored, accessed, and used.
- The LRS must provide a well-documented RESTful API calls.
- The LRS vendor must provide a name and contact information for the person responsible for privacy at their organization.

Browser Requirements

- The LRS should be compatible with the current version and last two major versions of Mozilla Firefox.
- The LRS must be compatible with the current version and last two major versions of Google Chrome.
- The LRS should be compatible with the current version and last two major versions of Apple Safari
- The LRS must be compatible with the current version and last two major versions of Microsoft Edge.
- The LRS must not require persistent cookies.
- The LRS must enable any required cookie to expire upon logging out, closing the browser or after a configurable timeout period.

- The LRS must not require any plugins, including but not limited to ActiveX, JRE or other Java plugins

Throughput Requirements

- The LRS must support minimally 60,000 average concurrent users.
- The LRS must be scalable to support up to 100,000 peak concurrent user data record streams.
- The LRS should support minimally 350,000 active user data record streams
- The LRS should be scalable to support 1,000,000 or more total user data record streams
- Performs with minimal latency under a variety of use case scenarios and load conditions
- Handles user data load efficiently, provisioning and scaling resources to smoothly accommodate fluctuations (especially spikes) in volume of statements sent to it.

4.1.1.2 Use Case #1 - Sample Evaluation Criteria

Acquisition of an LRS hinges largely on its ability to securely receive data from other systems in the environment. DoD Components may have certain processes and requirements, such as FedRamp, that must be followed. It is important to know if it is possible to perform acquisition of a product that doesn't yet meet such standards but could as a part of the acquisition process. The return on investment of a product that is already meeting requirements versus one that doesn't and would require the extra effort should be calculated by a DoD Component.

Once those requirements are met, the top LRS considerations are as follows:

1) Ability to protect and secure data. While meeting a high-level requirement is important, the product itself needs to have safeguards in place.
2) Talent consultancy/support with the product. A qualified individual(s) who can provide reach back, act as a sounding board, and allow organizational vicarious learning is important to have available to help figure out all the unknowns associated with any acquisition.
3) Robust and capable dashboards and analytics, while under consideration as a separate product, have the best results if integrated. Having the ability to store the data and then later references it allows some shortcuts that wouldn't use xAPI, even though it could. Flexibility is extremely important in dashboards and analytics.
4) The ability to effectively migrate data in the event of a transition between platforms through Data Portability.

4.1.2 Use Case #2 - xAPI Learning Content Acquisition

Learning content conformant to xAPI will often need to be developed as a part of an acquisition. The old paradigm of a content package and a content system being the only two components in a distributed learning solution is no longer valid. xAPI relies on an LRP taking responsibility for communication to an LRS. This means the LRP must create and send statements. Creation can simply be copying these directly from the content it is running but is the responsibility of the LRP, nonetheless. Before accepting ANY xAPI content, a strategy for that content working with an LRP must be in place. Often the LRP role is filled by an LMS, which a user is authenticated to, courses are registered for, and learning records can be sent from.

Data from xAPI content should be highly directed. It must follow the format of the xAPI specification but if it doesn't follow xAPI Profiles, it will have interoperability issues outside of the implementing organization and possibly even within when combined with other xAPI data sources. Organizations should supply or work with those creating content to define specific narrative-based xAPI Profiles and then align to existing xAPI data and profiles wherever possible.

While most xAPI properties have flexibility in the xAPI specification 1.0.3, some practices allowed by the specification will produce data interoperability issues. Many of these issues exacerbate the need for an LRP in place that can adequately modify "Statement Output" from a learning content to be ready for LRS consumption.

4.1.2.1 Use Case #2 - Sample Acquisition Language

- Learning content of any granularity that includes xAPI support shall have a specific and documented connection to an LRP that will be under the DoD Component's control. The Learning Content is still responsible for sending valid data to an LRP, even if the LRP converts it in any way into an xAPI Statement before sending it to an LRS.
- Learning content of any granularity that includes xAPI support or the LRP it is communicating with shall send Statements with ids that are globally unique. Contractors should work with DoD Components to determine a strategy for producing globally unique IRIs. This strategy should include base IRIs that are organizationally specific and then ensure uniqueness of the other IRI components. Learning Content on its own should not be performing lookup functions to determine statement id uniqueness.
    - The following IRI pattern should be adopted by anyone creating new concepts for a profile: https://w3id.org/xapi/ [profile name] / [concept type] / [concept]. IRI authors should only customize the content in the IRI in brackets. For example, the Video Profile Verb, https://w3id.org/xapi/video/verbs/seeked, follows this pattern.
    - Many existing IRIs/concepts do not follow this pattern due to legacy issues and that branching now would cause interoperability issues. They can be considered allowable exceptions to the requirement above.
- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with shall send Statements with Activities with unique IRIs. Contractors should work with DoD Components to determine a strategy for producing globally unique ids. This strategy should include base URIs that are organizationally specific and then ensure uniqueness of the other URI components. The following requirements/process from Navy Education and Training Command (NETC) is one such interpretation that follows all xAPI specification requirements that creates an IRI that begins with "https://":
    - The Activity ID shall not include any spaces.
    - An Activity ID shall not end with a trailing slash "/" unless the slash is required to resolve to the URL of an external resource.
    - For an Activity that is a link to an external resource (such as an external website) use that resource's URL as the Activity ID. This requirement only applies to external links.
    - The Activity ID shall not include a file name extension or the location of a file as part of the ID unless it's required to resolve to the URL of an external resource.

    - The Activity ID shall not include any URL-encoded characters unless it's required to resolve to the URL of an external resource.
    - For all other types of activities, an Activity ID shall include a Universally Unique Identifier (UUID) at the end of the IRI to make the Activity ID unique.
    - Do NOT use multiple Activity IDs to represent the same Object or reuse the same ID to represent different activities.
    - DoD Components shall maintain an inventory list of Activity IDs used for each project order to avoid causing Activity ID collisions by accidentally creating and using the same Activity IDs for different activities. The Activity ID inventory list is a required deliverable
    - Follow the above guidance for other ids, as appropriate.
- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with shall send Statements with timestamps. In addition, these timestamp values should be in Universal Coordinated Time (UTC).
- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with should send Statements with Actors that use the account/homepage mechanism for identification. Contractors should work with DoD Components to determine a strategy for supplying the correct Actor information based on authentication/permission to use the content. In addition, the homepage shall include a base URI that is specific to that DoD Component and under that DoD Component's control.
- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with shall implement the following xAPI Data specific requirements, unless a specific exception is made and documented (credit to NETC Guidance):
    - If the Actor is a learner, set the actor.objectType property with the value set to "Agent" unless defined differently in a specific xAPI Profile.
    - Set the verb.id to the identifier associated with the relevant Verb.
    - Set the verb display to the human-readable, past tense representation of the Verb.
        - include a display string in English with the language code of "en".
    - Set the object.definition.name to the language map value that represents the official name or title of the Activity.
    - Set the object.definition.description to the text value that represents a short description of the Activity.
    - Set the object.definition.type to the identifier associated with the relevant Activity Type.
    - The ID of the xAPI Profile (as an Activity) that a Statement is intended to conform to SHALL be declared in the category array within the context.contextActivities Object. Additional Profile Activity IDs for each Profile SHALL also be declared in the category array.
    - The registration property is used to identify multiple xAPI Statements that are all part of a particular attempt. The value of the registration property shall be a Universally Unique Identifier (UUID) and should persist throughout all Statements during each attempt.
- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with should send Statements that conform to Statement Templates of known and relevant xAPI Profiles whenever possible. Statement Templates can be found at https://profiles.adlnet.gov/.
- If new xAPI vocabulary is needed to successfully implement xAPI in the Learning Content, the DoD Component/Contractor should attempt to incorporate it into an xAPI Profile. Guidance for

xAPI concept and profile creation should be followed at https://adlnet.gov/guides/xapi-profile-server/user-guide/Profiles.html#profile-creation.

  - If the intended function of an xAPI Verb is slightly different from an existing verb, or additional information is needed, use the xAPI properties context, result, extensions, or other xAPI mechanisms to add this data to the Statement.

- Learning Content of any granularity that includes xAPI support or the LRP it is communicating with shall not send Statements that contain properties that are not either a) specifically in the xAPI specification/standard or b) created as an extension as defined in the xAPI specification/standard.
- DoD Components shall enforce this DoDI 1322.26 requirement "Content repositories within the DoD shall be leveraged whenever possible to re-use existing content, whether it be for legacy deployment or modernization to new web standards. Critical to reuse is that DoD Components acquire source files and other software components for each acquisition in accordance with DoDI 5000.87, dated 2 October 2020."
- Statements should not be communicated to the LRS using Basic Authentication directly from a web-browser.
- LRS credentials and the xAPI payload should not be accessible by learners.

4.1.2.2 Use Case #2 - Sample Evaluation Criteria

When evaluating criteria for content development, it is important that fulfilling all the pedagogical requirements come before technology-based criteria. The following criteria are valuable to determine ROI on developed content:

- Solid IRI design in Statements
- Data conformant to xAPI Profiles whenever possible
- In tools, Out-of-the-box capability for insightful data visualizations related to learner activity
- Past performance -Look at reviews from previous customers/contacts
- A cohesive data plan for all tracked data
- Recommended visualizations that are provided out of the box and other innovative/new uses of xAPI
- Select with future work in mind as far availability
- Determine if other APIs can be leveraged

4.1.3 Use Case #3 - xAPI Authoring Tool Acquisition

While it is possible to acquire an LRS for standalone purposes due to eventual capabilities not yet being acquired, this use case focuses on aligning and configuring all systems in a current environment to the newly acquired LRS.

An authoring tool does not function as an LRP. The same requirements of Learning Content Acquisition apply to xAPI Authoring Tools. The difference is that the expected output of an authoring tool is less likely to be modified (because there is an expectation it is published in a final form) than a normal content acquisition. Despite the likelihood, the output of an authoring tool SHOULD be held to at least the same level of scrutiny.

Certain functions should be baselined in an authoring tool. The tool should support the ability to apply different standards to content, or at least take in multiple formats of content and then apply xAPI. The authoring tool at a minimum must handle its own export formats and be able to change between them upon import. From a migration standpoint, being able to transform SCORM content to xAPI is extremely valuable. Tools should be extensible in allowing integrations with xAPI Profiles. Data validation of xAPI Profiles would be an extremely useful feature. An authoring tool that can import an xAPI Profile and then restrict the user appropriately is even better. Supplying direct access to both a code view and page layout view is very powerful.

4.1.3.1 Use Case #3- Sample Acquisition Language

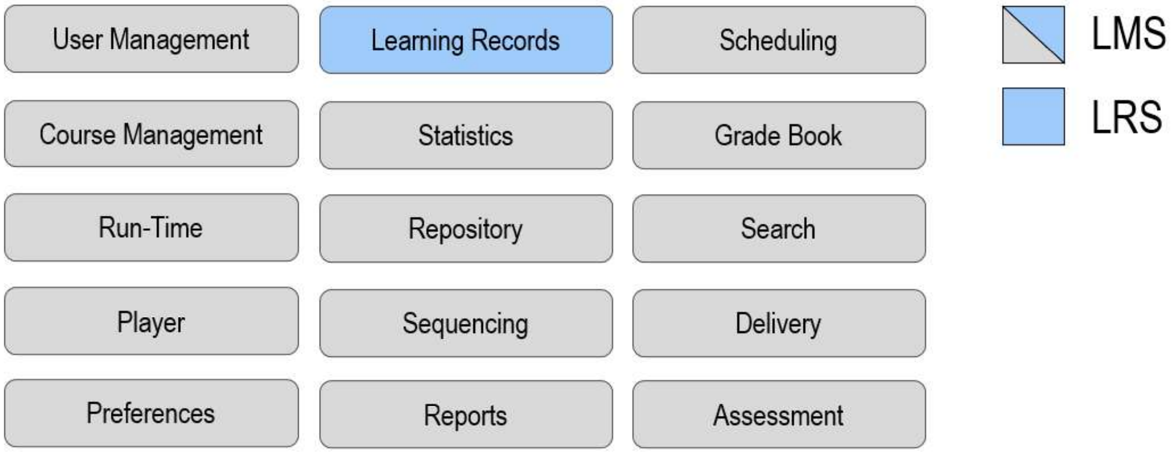
- An xAPI authoring tool shall create Learning Content that meets the criteria of Section 4.1.2.
- An xAPI authoring tool shall not create Learning Content with Statements that are restricted in the UI to a single choice (and otherwise not extensible) and also non-conformant to xAPI Profiles (Note that non-conformant is different from not being found in an existing xAPI Profile; Non-conformance is when a clear best practice has been defined, for example, for a verb and it is disregarded).
- An xAPI authoring tool should not create Learning Content with Statements that are restricted in the UI to a single choice and it otherwise not extensible.
- An xAPI authoring tool should not create Learning Content with Statements that are non-conformant to xAPI Profiles (Note that non-conformant is different from not being found in an existing xAPI Profile; Non-conformance is when a clear best practice has been defined, for example, for a verb and it is disregarded).
- An xAPI authoring tool should directly support the creation of Statements that align with xAPI Profiles. An xAPI authoring tool should directly describe which xAPI Profiles it can create.
- An xAPI authoring tool shall allow export, re-import of that exported content, modification of that content, and re-exporting of that content for the current version of xAPI.
- An xAPI authoring tool should allow the import of SCORM content and an export of xAPI content.
- An xAPI authoring too should allow validation of Statements/sets of Statements to a selected xAPI Profile
- An xAPI authoring tool should allow the selection of xAPI Profiles and then assist the development via UI restrictions based on that xAPI Profile.
- An xAPI authoring tool should allow direct access to both a code view and page layout view (if applicable).
- An xAPI authoring tool should allow the ability for multiple persons/roles to simultaneously access and work on Learning Content. Version control shall be supported in this case.

4.1.3.2 Use Case #3 - Sample Evaluation Criteria

Evaluation criteria for tools should focus on implementation of as many of the “should” requirements above as possible (“shalls” are non-negotiable). Interfaces should be simple but produce the desired results. The product shouldn’t require in-depth technical knowledge to apply standards.].

4.1.4 Use Case #4 - xAPI LRS Replacing an LMS

While it is possible to acquire an LRS for standalone purposes due to eventual capabilities not yet being acquired, this use case focuses on aligning and configuring all systems in a current environment to the newly acquired LRS. Figure 1 shows all of the capabilities that are traditionally filled by an LMS. A DoD Component will be aware of which of these are needed, but if looking to move to an LRS solution, should have a specific implementation strategy for determining a) LRP roles and responsibilities and b) all capabilities needed from Figure 1.



User Management	Learning Records	Scheduling
Course Management	Statistics	Grade Book
Run-Time	Repository	Search
Player	Sequencing	Delivery
Preferences	Reports	Assessment

Figure 1: LMS vs. LRS Capabilities

4.1.4.1 Use Case #4 - Sample Acquisition Language

At this time there is no "typical" case for replacing an LMS with an LRS, the capability sets are simply too different to suggest that a series of implementation details and requirements could provide predictable success. The suggested starting path to achieving such a migration may look as follows:

1. Determine and document the necessary functionality of the environment in its entirety.
2. Determine and document the functionality of the LMS.
3. Implement each of the functional components of the LMS in a web service or system.
4. Possibly done during step 3, possibly afterwards, instrument each web service or system with xAPI as LRPs

4.1.4.2 Use Case #4 - Sample Evaluation Criteria

Due to the unpredictable nature of such a migration, no evaluation criteria are appropriate. This would be a multi-step progress executed by the DoD Component and specifically acquisition.

4.1.5 Use Case #5 - LRS Dashboards/Analytics

The primary purpose of acquiring xAPI-based solution is to make informed decisions and to display data in meaningful ways. However, because of the modular nature of xAPI, these services are separate from the standard. While products in the legacy distributed learning era (e.g., LMS) relied on a specific integration, xAPI data is accessible as a part of the standard such that these components could be separate solutions. Most LRS products will include at least a baseline dashboards/analytics capability. It is recommended that those Services be considered separate of the other xAPI efforts and scored accordingly. A separate acquisition may be appropriate.

4.1.5.1 Use Case #5 - Sample Acquisition Language

- An xAPI Dashboard or Analytics Capability shall allow configuration of xAPI Statement extensions such that those vocabulary can be used.
- An xAPI Dashboard or Analytics Capability shall make a connection with the LRS that grants access to Statements based on permission.
- An xAPI Dashboard or Analytics Capability should leverage role-based creation and viewing of dashboards. At a minimum support senior leaders, instructors, subject-matter experts, instructional designers, and students.
- An xAPI Dashboard or Analytics Capability should integrate with outside data sources and be leveraged as a part of a data solution by applications, such as leaderboards, so that data can be aggregated even if not all explicitly stored in that LRS.
- An xAPI Dashboard or Analytics Capability should facilitate the ability to create and discover linkages with the specific learning content the learner experiences.

4.1.5.2 Use Case #5 - Sample Evaluation Criteria

Evaluation Criteria for dashboards and analytics should focus on implementation of as many of the “should” requirements above as possible (“shalls” are non-negotiable). Interfaces should be simple but produce the desired results. The product shouldn’t require in-depth technical knowledge to apply standards.

4.1.6 Use Case #6 - Multiple LRSs

This use case focuses on aligning and configuring multiple web services within an environment to different LRSs. Note that this does not mean multiple distinct LRS products are needed. The LRSs can exist in different configurations, security enclaves, and would be on distinct web infrastructure.   LRSs can be considered distinct for a variety of reasons, most of which stem from the need to separate data for security or efficiency. The same LRS can be configured to multiple “end points” (or resource locations) where xAPI data can be sent. By using some sort of data configuration service, xAPI data can be properly routed from one LRS to another based on rules. This service is currently beyond the scope of xAPI but is a highly recommended service for xAPI LRs.

4.1.6.1 Use Case #6 - Sample Acquisition Language

- For environments requiring at least one primary (meeting this requirement makes it primary) LRS, the primary LRS shall have ability to be configured to connect to multiple third party LRSs for, forwarding, filtering, and routing downstream.
- A learning environment should support dynamic communication between multiple LRSs (e.g. noisy, transactional, authoritative LRSs) as defined in the ADL Total Learning Architecture.
- A multi-LRS solution shall be able to configure multiple endpoints and send data between those “LRSs” via endpoint or other agreed-upon solution with the DoD Component.

- Each single LRS solution should be able to import and export Statements in bulk/totality to another LRS.
- LRS solutions should have both UI and API support for the transport mechanisms described in this section.

4.1.6.2 Use Case #6 - Sample Evaluation Criteria

Evaluation criteria for multi-LRS solutions (or even those considering future environment capabilities) should focus on implementation of as many of the "should" requirements above as possible.

4.2 Related Policies and References

- DoDI 1322.26 - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132226_dodi_2017.pdf?ver=2017-10-05-073235-400
- DoDI 1322.26 Reference - https://adlnet.gov/policy/fungible/
- DoDI 8320.02 - https://irp.fas.org/doddir/dod/i8320_02.pdf
- xAPI 1.0.3 Specification - https://github.com/adlnet/xAPI-Spec
- ADL Initiative's xAPI Project Page and Resources - https://adlnet.gov/projects/xapi/
- IEEE 9274.1.1 Open Source Landing Page - https://opensource.ieee.org/xapi
- IEEE 9274.1.1_202**2**_D1 - https://opensource.ieee.org/xapi/xapi-base-standard-documentation/-/tree/main
- xAPI Profile Server **-** https://profiles.adlnet.gov
- xAPI Accreditation Report, Impact of 1.0.3 to 2.0 https://adlnet.gov/assets/uploads/ADL%20xRAP%20Final%20Project%20Report.pdf
- Navy Guidance for xAPI Implementation - https://netc.usalearning.net/xapi-library/all-resources.html
- ADL's Hosted Prototype Learning Record Store - https://lrstest.adlnet.gov
- ADL's xAPI Adopters - https://adopters.adlnet.gov
- SCORM to xAPI Wrapper - https://github.com/adlnet/SCORM-to-xAPI-Wrapper
- xAPI Profile / Profile Server Guidance - https://adlnet.gov/guides/xapi-profile-server/user-guide/Profiles.html#profile-creation
- xAPI Developer Resources - https://veracity.it/xapi_developer_ultimate_resource_list_1

4.3 Recommended Best Practices

- In the event of a transition, ensure there is a plan to execute with disruption minimalized and data loss prevented.
- In advance of acquisition and Authority to Operate (ATO), there is significant value in having a PII-free, non-FedRamped (e.g., no ATO) space to test and prototype proofs of concept. This is not only for technical solutions of systems, but also management of data, analytics, and visualizations.
- Finalize version support of xAPI using the xAPI Accreditation Report as a guide.

4.4 Pitfalls to Avoid

- Be aware that security considerations can greatly impact anticipated start times/schedules. Having conversations with IT and Integration Teams is key.
- The "TinCan" packaging and other mentions of "TinCan" are not substitutes for xAPI or cmi5. TinCan was the early name given to the xAPI Specification when it wasn't a documented specification on GitHub. Protocols were created to ensure it was possible. Some of those tech pieces were picked up by Vendors and put into products. Learn more about these differences at https://aicc.github.io/CMI-5_Spec_Current/tincan/.
- Buying an authoring tool or content that is conformant/compliant with xAPI is not enough. To achieve data interoperability, an authoring tool should adopt specific xAPI profiles and document them as such. The most important of these profiles is cmi5.

4.5 Cybersecurity

As xAPI is a web service-oriented standard that involves communication across defined systems, it is fitting that cybersecurity practices are established for the use of this standard. Cybersecurity, as currently scoped in this document, doesn't necessitate guidance for xAPI Profiles as they are simply possible data points in the overall matrix of possible data points. While cmi5 does define specific communication protocols, these are also in the realm of possibilities of xAPI and are covered in this section. This guidance is expected to grow over time.

Since 2020, an IEEE Working Group has met to work on a set of *Recommended Practices for Cybersecurity in the Implementation of xAPI*. Although still in early draft, it is scoped as follows:

- The recommended practice document defines terms, including stakeholder types.
- The recommended practice documents how secure xAPI implementation fits into the broader category of best practices in cybersecurity.
- The recommended practice document discusses xAPI-specific cybersecurity best practices.
- The recommended practice provides use cases illustrating cybersecurity practices as relate to xAPI implementations.

In the same time period, ADL worked with a research team to establish an LRS Accreditation Project to identify the potential cybersecurity vulnerabilities or accreditation challenges and address these challenges through updates to the xAPI standard and by providing resources that support the accreditation process for xAPI-enabled education and training systems. The final report of this project can be found here.

Because the xAPI data model itself is open source, standardized, and transparent, it is easy to assess the risk posed by the inclusion of attributes communicated via xAPI. The data model itself poses no specific risk as compared to any general data model supporting any RESTful web service — in fact, the open nature of xAPI is a mitigating factor against the "black box" issue often faced by implementing other data models. Cybersecurity considerations regarding xAPI therefore should prioritize analyzing the risks inherent in products implementing xAPI and communicating xAPI data as opposed to over-analyzing the risk of the xAPI data model itself.

4.5.1 Cybersecurity-related Policies and References

From the point of view of the IEEE, the following cybersecurity policies and standards were identified.

IEEE P7002

https://standards.ieee.org/project/7002.html

“This standard defines requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data.”

IEEE P7004

https://standards.ieee.org/project/7004.html

“This standard provides stakeholders with certifiable and responsible child and student data governance methodologies.”

IEEE P7004.1

https://standards.ieee.org/project/7004_1.html

“This recommended practice produces best practices for meeting the requirements of IEEE P7004: Standard for Child and Student Data Governance when designing, provisioning, configuring, operating, and maintaining an online virtual classroom experience for synchronous online learning, education, and training.”

IEEE P7005

https://standards.ieee.org/standard/7005-2021.html

“This standard defines specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data.”

IEEE P7012

https://standards.ieee.org/project/7012.html

“The standard identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines.”

IEEE P9274.1.1

https://standards.ieee.org/project/9274_1_1.html

“This Standard describes a JavaScript Object Notation (JSON) data model format and a Representational State Transfer (RESTful) Web Service Application Programming Interface (API) for communication between Activities experienced by an individual, group, or other entity and a Learning Record Store (LRS).”

IEEE P9274.2

https://sagroups.ieee.org/9274-2-1/

“This Standard describes a JSON-LD format that defines concepts, templates and patterns of learner experience data.”

NIST Risk Management Framework (NIST)

https://csrc.nist.gov/projects/risk-management

“The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA).”

ADL xAPI Accreditation Guide

https://adlnet.gov/projects/xapi-rmf-accreditation-project-xrap/

“DoD cybersecurity policies state that any system that stores or transmits information must abide by certain cybersecurity requirements found under the RMF and codified in DoDI 8500.01. This project is evaluating current accreditation efforts for xAPI-enabled learning systems under RMF and developing guidance (e.g., suggested policy updates and Security Technical Implementation Guides or STIGs) to support xAPI-enabled system accreditation across DoD networks. The technical guidance produced under this project conforms to NIST guidelines and Defense Information Systems Agency accreditations required to deploy xAPI conformant solutions across the DoD.”

Hernandez, M., Neeley, M., Johnson, A., (2019). Cybersecurity Strategies for Accrediting

Experience Application Programming Interface (xAPI). Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).

4.5.2 Specific Cybersecurity Findings

The following findings can be used to influence acquisition decisions and language:

- An LRP must have some control over the content system or be trusted by the content system to complete the handshake necessary for communication.
  - If not, it means there is no reliable way to manage a registration between an LRP and LRS. This leads to workarounds which introduces security risks ranging from the ability to simply scrape the LRS credentials from the LRP to the ability to impersonate the authorized LRS.
- When an LRP-to-LRS communication exists (which is normal in xAPI) and the LRP contains an unsecure connection or unencrypted description of the LRS connection inside of it, it introduces risk as the data from the LRP could be trusted by the LRS but not secured.

    - Secure data communication from the LRP to the LRS should require Transport Layer Security — meaning established cryptographic protocols which allow the implementer with a means of attaining communications security over the network. This includes both encryption in transit and storage encryption at rest.
    - Solid network practices should include either keeping the LRS internal to the local private network of the LRP or creating a secure tunnel between the two.
- When using xAPI and considering transport-level security (the security of the external interface of an LRS), the implementation strategy below will help to mitigate or prevent message interception, Man-in-the-Middle attacks, message/statement alteration at the time between LRP and LRS. The implementation strategy consists of:
    - Strong signing algorithm SHA-256
    - Strong key exchange (Elliptic-Curve Diffie-Hellman)
    - HTTPS (For example, HSTS with long duration, including subdomains and preload directive).

5.0 CMI5

cmi5, which is not an acronym, rather a name that pays tribute to the historical “computer managed instruction” models, is considered to be the first and most basic xAPI Profile that is designed to update the current SCORM paradigm. While it technically is more than the xAPI Profile as defined by the xAPI Profile Specification, the concept of an xAPI Profile being additional rules and requirements is still true. These requirements are all centered around a learner’s interactions with learner content through a LMS. cmi5 cannot be implemented without xAPI. It is recommended for any LMS-based solution that both are implemented together.

5.1 Use Cases

The use cases in this document are organized to be simplistic and categorical, such that they can be building blocks for creating high quality acquisition language. In this way, a set of use cases can be used to match as closely as possible to an organization’s requirements. Subsets of use cases will be listed under each use case section as a bullet.

The use cases for cmi5 include the different products (LMS, content, authoring tools) that would support cmi5 and different migration-based approaches that are likely to be encountered. These approaches are designing for cmi5 data in non-cmi5 systems, cmi5 without an LMS, and cmi5 with multiple LMS/LRS support.

Each use case in a subset will contain several format-specific or domain-specific high-level requirements. It will contain instructions on how the technology can meet those requirements, and is a value proposition to the learning environment.

In the subsequent sub-section under each use case, sample acquisition language will be provided and will be structured with the purpose of mirroring the use cases directly. Every use case has corresponding sample acquisition language. In this section, there will not be a one-to-one correlation and will instead focus on categories that are introduced, such as “if deploying a competency-based strategy”. At this time, no previously used contract language can be used, and thus will not be quoted.

As a key effort in cmi5 adoption and bridging the gap between SCORM and other pre-xAPI technology to xAPI, The ADL Initiative launched the CATAPULT effort. The software, open-source code, documentation, and course templates from that effort should be leveraged whenever possible.

5.1.1 Use Case #1 - cmi5 LMS Acquisition

An LMS performs many functions as a software system that includes many Web Services. The cmi5 specification only defines a few of these functions and is itself agnostic to the rest. This document will not describe the “shall” requirements in the cmi5 specification as they are captured in the specification and tested through the conformance test suite. Due to the critical nature of ensuring the test suite is run correctly, that contract language will be included in 5.1.2. The functions that the LMS is expected to perform within cmi5 are as follows:

- Content Launch Mechanism
- Authentication
- Session Management
- Reporting
- Course Structure

An LMS is typically the central hub of authenticated learner activity. As such, it ties into other services and capabilities. The LMS Administrator is a key role that was not considered in previous standards, such as SCORM. In many use cases, direct intervention of an LMS Administrator on behalf of a learner is necessary. Those interventions cannot break data implementations of standards. The following use cases describe LMS responsibilities and in some cases, where an LMS Administrator may need to be involved:

- Use of Objectives and/or Sequencing. While much of competency-based education is beyond the scope of cmi5, the specification does support “tagging” in the course structure format. An LMS may wish to use this for integration. Similarly, if a substitute for SCORM sequencing is needed, cmi5 does have a best practice for defining it. **Cmi5 conformance testing does NOT include sequencing for this version of cmi5 (Quartz).**
- The LMS needs to be accountable to how URLs and session management are handled, in particular, when the learner makes progress. In cmi5, the URLs in session management are handled through URLs and “moveOn” criteria.
- An LMS that can provide mobile support can support cmi5 in that capability.
- The LMS needs to take all necessary steps to validate the actor. While there are multiple ways to do this, best practices have been found.
- There are times when the criteria for success in a course/AU is different for various learners. This is accomplished through the use of Mastery Score.

5.1.1.1 Use Case #1 - Sample Acquisition Language

- An LMS shall be xAPI compliant as described by all requirements in Section 4.
- An LMS shall pass the “cmi5 LMS Test Suite” within the overall CATAPULT conformance test suite software as available at https://github.com/adlnet/CATAPULT and as documented at

https://adlnet.github.io/CATAPULT/ . LMS Vendor shall supply logs of the completed test and should supply a live or recorded demonstration of the Test Suite passing. If an LMS is versioned or a different version is being acquired, the Vendor shall supply new logs and if possible, demonstrations. This is not a significant technical burden as the process is largely scripted, and an LMS producing such a script once will likely see it completely reusable.

- If an integration is being pursued instead of a product, then the following language could be appropriate: "An LMS shall integrate with the CATAPULT Player Prototype by leveraging code within it to reduce time/effort of acquisition."
- An LMS should meet as many of the "should" requirements as documented in the cmi5 specification (https://github.com/AICC/CMI-5_Spec_Current/blob/quartz/cmi5_spec.md) as possible. DoD Component should request documentation from LMS Vendor regarding all such requirements, their product's implementation or lack of implementation, and rationale.
- Unless a DoD Component finds an exception to its current and future requirements of sequencing, an LMS shall implement the cmi5 Extensions as described at https://aicc.github.io/CMI-5_Spec_Current/extensions/. This currently includes "requires" and "collateralCredit" as supported extensions to a course structure format. This is critical because if an LMS doesn't support the extension, content authors and tools cannot use them.
- An LMS should not attempt to correct bad data and instead reject the bad data in accordance with xAPI/cmi5 requirements.
- DoD Components should work with a product Vendor to ensure cmi5 Objective support aligns to any existing competency-based education or Competency Framework support, if applicable.
- An LMS shall implement the returnURL as described in the cmi5 specification.
- An LMS shall follow all "Fetch URL" in the cmi5 Best Practices, as follows (the two "should" requirements shall be followed unless a better solution is documented and agreed upon by DoD Component and Vendor):
  - "The Fetch URL must be unique for each session.
  - The Fetch URL must only return an auth token on the first call. (Subsequent calls must return an error – i.e. it must be a "one time use" URL)
  - The Fetch URL must not reuse auth tokens.
  - The Fetch URL should return a 4xx HTTP error if an HTTP method other than POST is used.
  - Since the Fetch URL can only be called once, the auth token should be stored in non-volatile storage (see best practice "Persist AU Session State")"
- An LMS supporting mobile should consider one of the following options of cmi5 implementations when an AU is considered a mobile app.
  - Option 1: Use an app protocol in the launch URL.
    - AU is an app.
    - AU has URL with a protocol LMS launches App using URL with app protocol.
    - An app redirecting to browser is not useful. If using app protocol to launch, don't use "returnURL".

  - Option 2: Use an HTML wrapper to launch the app AU is an HTML page (wrapper) that directs from the mobile browser to the app.
- An LMS shall reject Statements that do not conform to cmi5. Another way of describing this requirement is that if a Statement is attempting to be "cmi5-defined" per Section 7.1.3 of the cmi5 Specification and not following requirements of the specification, it shall be rejected. DoD Component and Contractor/Vendor should discuss the specific implementation details of fulfilling this requirement. This does not mean that Statements from other xAPI Profiles should be rejected, as these are examples of cmi5-allowed Statements. Statements that are considered "cmi5-not allowed" shall also not be rejected, and the DoD Component and Contractor/Vendor should have a strategy on how to handle/route those data. Unless a specific exception is granted by the DoD Component, an LMS shall not correct data from an AU in lieu of rejecting that data.
- An LMS shall support use of the "progressed" verb in support of the data requirement below:
  - "For recording progress during a session, it is recommended to use a cmi5 allowed statement with the progressed verb (http://adlnet.gov/expapi/verbs/progressed) and a progress extension in the result (see section 9.5.5.1 of specification). Progress statements should not be sent for progress value of 100% as that indicates completion. Once the learner reaches 100% it is recommended that a cmi5 defined "completed" statement be issued instead."
- An LMS shall create satisfied Statements in the following way:
  - LMS creates a cmi5 "allowed" statement (with a satisfied verb) when an AU has met its moveOn criteria. The statement should also include the same AU activityId used in cmi5 defined statements.
- An LMS shall reject with an HTTP 403 a Statement if the Session ID, authorization token, actor in statement, and actor do not match. This verifies that the Actor in the statement matches the actor provided on the launch URL and that the authorization token provided was the same one issued for that specific launch session.

5.1.1.2 Use Case #1 - Sample Evaluation Criteria

The following criteria should be considered when considering a cmi5 systems:

- The capability to integrate directly with CATAPULT for testing will establish a pipeline for continued checks on conformance
  - Open APIs that allow cmi5 if not directly supported (meaning not every LMS action needs to have a UI component)
- The capability to leverage Open APIs for other functions
- The system leverages a version of LTI that allows integration with existing systems
- The ability to augment an existing system with CATAPULT could be a very large ROI and should be considered in solutions in addition to acquisition of full products

5.1.2 Use Case #2 - cmi5 Content Acquisition

The cmi5 specification creates a clean hand-off between content and system. Using xAPI alone has many challenges. There is no need to determine what an LRP's responsibility is in cmi5 because the brokering is handled by the LMS by the specific way any cmi5 content, in the form of AUs, interacts with it.

Testing is extremely important in content acquisition. The cmi5 Test Suite provides the ability to launch cmi5 content packages, create logs of their conformance, as well as xAPI data generated. Data is also sent to an LRS in a more complete form. These tests are important, but end user tests within the end environment are also important. Usability testing does not currently have supporting software.

An AU developer often acts as the Subject Matter Expert and may implement such behaviors in that AU. AUs should be created diversely and with diverse xAPI data that goes beyond cmi5, as appropriate. As in xAPI, there are data properties that need to be adequately defined. cmi5 provides most of that definition. Lingering factors include lining up the Actor with the LMS account, creating unique identifiers for activities, and creating effective Statement ids and timestamps. Many of these requirements are specific in the cmi5 specification but are articulated here for importance and in alignment with the xAPI requirements.

An AU Developer will produce Content, which consists of both AUs and the Course Structure Format that accompanies the AUs, as well as their collective role as a Content Package.

The following use cases describe Content responsibilities:

- Use of Objectives and/or Sequencing. While much of competency-based education is beyond the scope of cmi5, the specification does support “tagging” in the course structure format. Similarly, if a substitute for SCORM sequencing is needed, cmi5 does have a best practice for defining it. **Cmi5 conformance testing does NOT include sequencing for this version of cmi5 (Quartz).**
- The AU can respond to a mastery score issued by the LMS. This could be by design of the course as the AU author intended or could be from an LMS Administrator intervention.
- A Course Structure creator needs to specify moveOn criteria.
- An AU needs to handle when a returnURL is not provided.
- An AU needs a reliable way to track progress through an xAPI Statement.
- An AU creating Statements should maximize their value and discoverability by using connecting it to the registration.
- An AU needs to match cmi5-defined and cmi5-allowed Statements’ Actor properties to that in the launch URL as an LMS will reject otherwise.
- An AU should use cmi.interactions (a part of the xAPI specification) in an interoperable way.
- An AU should be designed to preserve the state of following operations that have been performed in the case where an operation may break the session when it was not intended.

5.1.2.1 Use Case #2 - Sample Acquisition Language

- Consider all requirements from Section 4.1.2.1 where conflicts with cmi5 do not arise.
- DoD Components and contractors prior to content delivery shall use the CATAPULT Test Suite and provide logs of both the Statements generated and success/failure of the content. Analysis

of the data sent to the LRS shall also be done to align to agreed-upon requirements, as appropriate.

- DoD Components and contractors prior to delivery shall test cmi5 content in an environment as close as possible to the end-user environment (cmi5 LMS). If the end-user environment is not available for this purpose, then use the cmi5 Player, such as the open-source player provided by the ADL Initiative, to demonstrate the cmi5 courseware's functionality.
- AUs act as the LRP and follow all rules within the cmi5 specification to achieve that role.
- AUs shall send Statements with ids that are globally unique. Contractors should work with DoD Components to determine a strategy for producing globally unique ids. This strategy should include base URIs that are organizationally specific and then ensuring uniqueness of the other URI components. AUs should not be performing lookup functions to determine statement id uniqueness.
- AUs shall send Statements with Activities with unique IRIs. Contractors should work with DoD Components to determine a strategy for producing globally unique IRIs. This strategy should include base IRIs that are organizationally specific and then ensuring uniqueness of the other IRI components.
- AUs shall send Statements with timestamps. In addition, these timestamp values should be in Universal Coordinated Time (UTC).
- AUs shall only create and send Statements with Actors that use the account/homepage mechanism for identification. Contractors should work with DoD Components to determine a strategy for supplying the correct Actor information based on authentication/permission to use the content. In addition, the homepage shall include a base URI that is specific to that DoD Component and under that DoD Component's control.
    - "The "Actor" field should be traceable back to a learner's DoD ID. The recommended solution is to use the DoD ID as the "Name" property under the Actor's "Account" property." (DoDI 1322.26)
- AUs creating and sending cmi5-allowed Statements or non-cmi5 Statements in an otherwise cmi5 solution should conform to Statement Templates of known and relevant xAPI Profiles whenever possible. Statement Templates can be found at https://profiles.adlnet.gov/.
- Use of Objectives and/or Sequencing. While much of competency-based education is beyond the scope of cmi5, the specification does support "tagging" in the course structure format. Similarly, if a substitute for SCORM sequencing is needed, cmi5 does have a best practice for defining it. **Cmi5 conformance testing does NOT include sequencing for this version of cmi5 (Quartz).**
- The AU can respond to a mastery score issued by the LMS. This could be by design of the course as the AU author intended or could be from an LMS Administrator intervention.
- A Course Structure creator must specify moveOn criteria.
- An AU needs to handle when a returnURL is not provided.
- An AU needs a reliable way to track progress through an xAPI Statement
- An AU creating Statements should maximize their value and discoverability by using connecting it to the registration
- An AU needs to match cmi5-defined and cmi5-allowed Statements' Actor properties to that in the launch URL as an LMS will reject otherwise

- An AU should use cmi.interactions (a part of the xAPI specification) in an interoperable way
- An AU should be designed to preserve the state of following operations that have been performed in the case where an operation may break the session when it was not intended.
- The DoD Component shall, for the sake of this requirement, be considered the government project lead in evaluation of this DoDI 1322.26 requirement - "Prior to developing a course, the vendor or government project lead shall determine which xAPI Profile(s) to use, as well as the associated vocabularies and roll-up rules that determine how the xAPI data will be aggregated to support assessment. Failure to adequately address data interoperability will lead to content that cannot be re-used."
- DoD Components shall enforce this DoDI 1322.26 requirement "Content repositories within the DoD shall be leveraged whenever possible to re-use existing content, whether it be for legacy deployment or modernization to new web standards. Critical to reuse is that DoD Components acquire source files and other software components for each acquisition in accordance with DoDI 5000.87, dated 2 October 2020."
- Statements should not be communicated to the LRS using Basic Authentication directly from a web-browser.
- LRS credentials and the xAPI payload should not be accessible by learners.

5.1.2.2 Use Case #2 - Sample Evaluation Criteria

The ideal content uses CATAPULT Templates for two purposes. First, for better interoperability and integration into cmi5 environments and second, to reduce the cost of development and cost in legacy content conversion. Evaluations should be done on the overall ROI of the content, which will be significantly higher the more reuse occurs. Content is typically done as a service-based contract, so optimizing development time, cost, and capability will ultimately produce more content.

5.1.3 Use Case #3 - cmi5 Authoring Tool Acquisition

The same requirements of cmi5 Learning Content Acquisition apply to cmi5 Authoring Tools. The difference is that the expected output of an authoring tool is less likely to be modified (because there is an expectation it is published in a final form) than a normal content acquisition. The nature of cmi5 is to produce courses, blocks, and AUs that are ready to be "plugged in" to cmi5 LMSs. Unlike with xAPI, cmi5 requirements are strict enough that authoring tool output is going to not require modification or configuration to be ready for a cmi5 LMS.

Additional requirements beyond the cmi5 specification have to do with interoperability, functionality, and usability.

5.1.3.1 Use Case #3 - Sample Acquisition Language

- "The solution must provide analytics capabilities with role-based dashboard and visualizations for different users throughout the enterprise."

5.1.3.2 Use Case #3 - Sample Evaluation Criteria

Tools that automate should be transparent in what they are changing and provide an audit trail to understand it. Manual ability to insert xAPI/manual code is important as it allows experts to finely-tune. Coding should have real-time error checking of xAPI/cmi5 Statements.

5.1.4 Use Case #4 - cmi5 Profile Data Only Approach (Pre-LMS Acquisition)

cmi5 cannot be considered adopted without an LMS or LMS set of services in play. However, cmi5 does contain an xAPI Profile as a set of its requirements. These data requirements can be adhered to until an LMS is acquired.

5.1.4.1 Use Case #4 - Sample Acquisition Language

- "The solution must provide analytics capabilities with role-based dashboard and visualizations for different users throughout the enterprise."

5.1.4.2 Use Case #4 - Sample Evaluation Criteria

The most important evaluation criterion is determining if LRS data is xAPI and cmi5 compliant. Anything short of this criterion is failing the use case.

5.1.5 Use Case #5 - LRS Dashboards/Analytics

The primary purpose of acquiring xAPI-based solution is to make informed decisions and to display data in meaningful ways. However, because of the modular nature of xAPI, these services are separate from the standard. While products in the legacy distributed learning era (e.g., LMS) relied on a specific integration, xAPI data is available as a part of the standard such that these components could be separate solutions. Most LRS products will include at least a baseline dashboards/analytics capability. It is recommended that those Services be considered separate of the other xAPI efforts and scored accordingly. A separate acquisition may be appropriate.

5.1.5.1 Use Case #5 - Sample Acquisition Language

- "The solution must provide analytics capabilities with role-based dashboard and visualizations for different users throughout the enterprise."
- A cmi5 Dashboards or Analytics Capability shall allow configuration of xAPI Statement extensions such that those vocabulary can be used.
- A cmi5 Dashboards or Analytics Capability shall make a connection with the LRS that grants access to Statements based on permission.
- A cmi5 Dashboards or Analytics Capability should leverage role-based creation and viewing of dashboards. At a minimum support senior leaders, instructors, subject-matter experts, instructional designers, and students.
- A cmi5 Dashboards or Analytics Capability should integrate with outside capabilities, such as leaderboards, so that data can be aggregated even if not all explicitly stored in that LRS.
- A cmi5 Dashboards or Analytics Capability should facilitate the ability to create and discover linkages with the specific learning content the learner experiences.

5.1.5.2 Use Case #5 - Sample Evaluation Criteria

Evaluation Criteria for dashboards and analytics should focus on implementation of as many of the "should" requirements above as possible. Interfaces should be simple but produce the desired results. Use of the product should not require in-depth technical knowledge.

5.1.6 Use Case #6 - Multiple LRS/LMS Support

This use case doesn't change pragmatically from Section 4.1.6. The fact that one of the LRPs is now a cmi5 LMS doesn't impact the requirements for multiple LRSs (even compliant LMSs that have compliant LRSs) to communicate with each other. No additional details from those provided in Section 4.1.6 are necessary for this use case at this time.

5.2 Related Policies and References

- DoDI 1322.26 - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132226_dodi_2017.pdf?ver=2017-10-05-073235-400
- DoDI 1322.26 Reference - https://adlnet.gov/policy/fungible/
- DoDI 8320.02 - https://irp.fas.org/doddir/dod/i8320_02.pdf
- cmi5 Working Group Page - https://aicc.github.io/CMI-5_Spec_Current/
- ADL Initiative's cmi5 Page - https://adlnet.gov/projects/cmi5-specification/
- ADL Initiative's Project CATAPULT (cmi5 Player and Test Suite) Page - https://adlnet.gov/projects/cmi5-CATAPULT/
- cmi5 Content Player, Test Suite, and Templates - https://github.com/catapult-project/catapult
- SCORM vs. cmi5 Comparison (by cmi5 Working Group) - http://aicc.github.io/CMI-5_Spec_Current/SCORM/
- cmi5 as SCORM Replacement Article - http://risc-inc.com/next-generation-scorm-cmi5/
- cmi5 Working Group / Landing Page - http://aicc.github.io/CMI-5_Spec_Current/
- cmi5 Overview - https://adlnet.gov/resources/cmi5-resources/
- cmi5 Code Library - https://github.com/adlnet/cmi5-Client-Library
- cmi5 Adopters List - https://aicc.github.io/CMI-5_Spec_Current/adoption/
- cmi5 Best Practices - https://aicc.github.io/CMI-5_Spec_Current/best_practices/
- cmi5 Worst Practices - https://aicc.github.io/CMI-5_Spec_Current/mistakes/
- cmi5 Code Library - https://aicc.github.io/CMI-5_Spec_Current/client/
- cmi5 Sample Statements - https://aicc.github.io/CMI-5_Spec_Current/samples/
- cmi5 Runtime Example video - https://www.youtube.com/watch?v=nhJRIDNE96Q
- cmi5 Process Flow - https://risc-inc.com/cmi5-overview-process-flow/
- AU Flow - https://aicc.github.io/CMI-5_Spec_Current/flows/au-flow.html
- LMS Flow - https://aicc.github.io/CMI-5_Spec_Current/flows/lms-flow.html

5.3 Recommended Best Practices

- The cmi5 Working Group has documented best practices at https://aicc.github.io/CMI-5_Spec_Current/best_practices/ - many of these were used in the use cases and sample acquisition language.
- Unless an equivalent cmi5 Adopters website to the xAPI Adopters website can be stood-up, the best known list of cmi5 Adopters can be found at https://aicc.github.io/CMI-5_Spec_Current/adoption/. DoD Components should consider this a starting point if searching out cmi5 Products and Services.
- DoD Components considering migration from SCORM should look at the following analysis: https://aicc.github.io/CMI-5_Spec_Current/SCORM/

5.4 Pitfalls to Avoid

- cmi5, like many standards, is based on data management and not on data security. It is expected that data security best practices change faster than data standards. Conformance testing for cmi5 may require certain security to pass tests, but it doesn't mean other security protocols or controls cannot be implemented.
- Basic Auth is not being used as a username/password encoding scheme in cmi5. Basic Auth (RFC 7235) was selected because it was the most widely used scheme at the time the xAPI specification was created. Basic Auth is used to provide a temporary "authorization" to the LRS (not authentication to the LRS). Authentication to the LRS is expected to be managed by the LMS or some other mechanism. With cmi5, a Basic Auth token is used in the HTTP header of xAPI requests made by the Learning Activity. Actual learner authentication is outside the scope of cmi5.
- "LMS" is used in cmi5 to differentiate between the system responsibilities that it has that are different from an LRS. It is very likely the same product would act as both an LMS and an LRS. The only characteristics that make a product an LMS in the view of the cmi5 specification are those that are documented as requirements. A minimal set of services may be needed to accomplish this, even to the point where it may not look like a traditional LMS.
- The "TinCan" packaging and other mentions of "TinCan" are not substitutes for xAPI or cmi5. TinCan was the early name given to the xAPI Specification when it wasn't a documented specification on GitHub. Protocols were created to ensure it was possible. Some of those tech pieces were picked up by Vendors and put into products. Learn more about these differences at https://aicc.github.io/CMI-5_Spec_Current/tincan/.

5.5 Cybersecurity

Cybersecurity for cmi5 follows the xAPI cybersecurity restrictions in Section 4.5. While other cmi5 profiles are not likely to introduce additional requirements, cmi5 is a special case in that its launch mechanism and authorization protocols must be met. As The ADL Initiative Research and Development team facilitates the cmi5 Player and Test Suite through cybersecurity processes, any issues that go beyond xAPI will be discovered and documented.

Note that while cmi5 does impose authorization requirements, it does not impose authentication requirements. Authentication of a user to a system is a prerequisite to using cmi5 and its launch and authorization. As the use of the cmi5 Player and Test Suite increases across DoD, additional cybersecurity measures will be reported in future versions of this document.

6.0 LEARNING METADATA

Historically, guidance for metadata within the DoD has been sparse. Legacy documents refer to the documentation of items within software architectures, which doesn't serve the distributed learning paradigm well. Distributed learning guidance simply pointed to the use of SCORM to solve metadata problems. SCORM was one of the few standards that proscribed certain mandatory and optional properties.

Due to the mandatory/optional nature of metadata specifications and standards, being conformant to such a standard can become trivial (e.g., implementing zero of the optional properties). However, forced conformance can become more damaging as many metadata creators did a poor job aligning metadata to content or simply put the required data in the fields as a gate to simply "check the box" for the standard. Some of this "box checking" was justified as some of the mandatory properties in SCORM were simply not useful for DoD use cases.

With these constraints in mind, an IEEE Working Group was formed in 2020 with the purpose of creating a metadata standard that could provide value to the DoD, such that every property was designed with a purpose of aligning to a specific DoD use case. P2881 doesn't refer specifically to courses or lessons, rather declares different scopes for Learning Objects. For the purposes of this document, ALL such content are Learning Objects unless a particular scope is provided. There is a current draft of the P2881 but due to IP issues, it cannot be shared until the standard is finalized. This document will refer to overall strategies and generic names of properties to support that standard but the final "names" of each property and potentially some of the exact data formats will have to be finalized either after the standard is published. Future versions of this document will spell out specific data requirements, such as "this property shall be populated with one of the following values: *value a*, *value b*, or *value c*."

Metadata implementations have historically relied on "records" of metadata, which traditionally were XML-based documents that contained all properties of that learning object and itself had an identifier. Current practices consist of another option that uses a graph-based structure with references such that every learning object, property, and values of properties are all in the same space and can cross-reference as a "web." This document recommends the use of a graph structure for metadata and many properties will function much more effectively and efficiently with its use. However, the guidance can be applied to both solutions.

6.1 Use Cases

This document contains only a single, large use case. The rationale is that the use case of tagging content for metadata will fulfill a variety of use cases and that properties themselves are no longer mandatory/optional, rather mandatory if certain functions are desired. Thus, all sample contracting language will be written in an "if/then" format. For example, if a Learning Object is to be discoverable via a text search, then use of the "keywords" property of P2881 is necessary.

When considering a metadata tagging strategy, a key question becomes "at what level of granularity should the DoD Component use when tagging a Learning Object with metadata?" In SCORM, these were typically asset, Shareable Content Object (SCO), which was akin to a "lesson", and the full course (content package). Assets are much more useful if a Learning Content Management System (LCMS) is used that already provides support to course creators in management of these objects for future creation. It is important to understand that a course is not simply the sum of its parts. Decontextualizing Learning Objects at the lesson level may not be as simple as removing them from a course as standalone. Take these into consideration when evaluating metadata use cases as this document will not recommend a "one size fits all" approach.

As competency-based education and the use of competencies increases to provide time and cost savings to DoD by optimizing time-on-task and other human performance measures, the alignment to Learning Objects cannot be understated. Regardless of the level of hierarchy, it should strongly be considered to tag any level of Learning Object that itself teaches or assesses a competency (see below for details).

6.1.1 Use Case #1 - Tagging Learning Content

This use case brings together a great number of reasons to "tag" content (populating metadata properties) and a description of how to use the P2881 standard and application profiles to execute that process. There are two primary roles that this use case serves a) a learner or system on behalf of a learner trying to match a learning opportunity to that learner and b) an instructional designer, developer, or curriculum manager looking for a Learning Object for the sake of locating and deploying/reusing it toward an eventual end user.

Sample acquisition language in the sub-section can be used to adequately provide the requirements and supplies the "if/then" language. Bullets in the sample acquisition language will correspond to the bullets in this section. The "if" in each of these bullets is to be considered the condition for ALL sentences/requirements within that bullet.

- Learning Objects are intended to be uniquely referred to both within and outside of the DoD Component. Whether this is a key in a database or a point on a graph, a unique and resolvable identifier is needed.
- Many tools use a basic matching algorithm to locate Learning Objects. The user interface for these basic searches use a single text box to capture search terms. Algorithms include different weights for different properties that are matched. An adequate number of properties to describe the resource generically are necessary.
- A user of a search-based tool will need to process the search results and have those results be structured in an understandable way. This is often the name of the Learning Object with some descriptive text. Often a UI will allow the user to click a link to more information (metadata), but curation by the user often uses basic information to decide which to obtain more information about.
- Further curation is required at the next "layer" down of information. This is where the user decides if the learning object is "right" for them based on additional relevant properties.
- Classification of Learning Objects by a subject area is a valuable way to adequately enable systems that understand their relevance. Using these classifications provides valuable context within the systems they are deployed within and often align to Competency Frameworks.
- Learning Objects are sometimes created for a specific audience. This can be a classification of people or a generic description of whom the Learning Object is intended to serve. Whether it is a

system that looks for a match of users to this classification or information the user gets to self-assess the Learning Object's audience to themselves, using this property can meet the use case.

- While Learning Objects can be created for an audience, sometimes there is a particular geographical or regional context that is required for intended use of that Learning Object. A property that allows a freeform expression of these contexts, which may or not be integrated with another service that adequately defines them, is necessary to meet this use case.
- Almost every Learning Object will have an audio or text component that has a particular language in which it is being delivered. A property is necessary to capture this language such that they or a system can make an informed decision whether it is appropriate for them or not.
- One reason that a single use case can accommodate so many requirements is the notion that a Learning Object can be tagged for its intended purpose using P2881 that wasn't previously used. By determining as a core concept whether a Learning Object is intended to be a static asset, a strategic learning component, or a deployed learning instance that requires resourcing (e.g., instructors, seat licenses), significant adjustments can be made to the UI/UX that a supporting system provides. By simply enabling this core concept, user flows can be specifically directed to meet their intended purpose of finding that Learning Object.
- Another core principle in defining a set of metadata properties is that when different properties are applied to Learning Objects, they behave very differently based on their native type. For example, a duration of a video is its run-time, but an online instructor-led course could be measured in weeks. In previous standards, these were lumped together in a single property, and it was left to a system to disambiguate. By defining a specific "type" to a Learning Object, communities of practice can establish particular properties that are important as an application profile.
- In a very similar way, extensibility is a very important part of metadata. Metadata should not be considered non-conformant if it has additional properties. By allowing extensibility through "types", all use cases can be met simply by defining the Learning Object as a unique type.
- Learning Objects are, unsurprisingly, designed with Learning outcomes in mind that can often be associated with gaining a competency. What makes a competency is beyond the scope of this standard's guidance. However, Learning Objects are often performing formative and summative exercise and evaluations. Not all Learning Objects do both (e.g., not all Learning Objects are courses, nor do they all both teach the content and evaluate the learner's progress in that content). It is important that Learning Objects can specify competencies that are both taught by the Learning Object and those that are assessed by it.
- Systems that use metadata will typically have role-based permissions that could directly tie into the lifecycle/publication process of Learning Objects. These permissions aren't specifically tracked by metadata, but an overall view of which Learning Objects are available to be accessed for the "normal" user is a versatile property that can be used both for pre-publication and for inactive "instances".
- When a system used role-based permission, there may be the need to restrict availability more deliberately by specific person, groups, or by labels. A property that allows the control of availability of that Learning Object only to authorized individuals is an important property.

- For both previous properties that have to do with availability, it does not mean that the metadata drives the system, nor does it mean that the system populates the metadata. However, one of these should be the case. To put it another way, the system is likely the manager of searches that would display based on availability. The metadata can either reflect what the system "knows" or those records can be changed by authorized individuals which effectively sets the permission of them as the system will "read" those records.
- To facilitate a ledger of versions of a Learning Object, keeping track of the revisions is extremely important. By keeping track of a previous and next version of Learning Objects within metadata, the most recent version can then serve to update all the previous versions, with all versions then "knowing" they are the latest. The value of this property does rely on either a LCMS capability to populate it on publication and/or the ability for the URI of metadata of the Learning Object to report/be subscribed to.
- A Learning Object could change drastically in that it wouldn't be considered simply another version. It could also be (legally) shared and then be changed by a different author, such that they would call it their own derived work. Properties that enable an audit trail like versioning is important to understand how much re-use has occurred and to allow derived works to "subscribe" to a version of a Learning Object that itself could be updated. For example, a course is freely shared and re-skinned and the assessment is changed, becoming a derivation. However, the original version of the course is updated by the original author due to updated doctrine. The DoD Component that acquired that course would appreciate knowing about that update and potentially using the new version. Properties that allow both the knowledge of what the Learning Object derives into and where it was derived from enable this function.
- At times, multiple forms of a Learning Object exist that have a common origin. However, these forms aren't derivations as they aren't necessarily drastic changes, they may just be different representations of that same Learning Object. Examples could be different formats of the same source material. In these cases, it isn't so much of keeping track of a list of versions, rather just the originating source material. Properties that allow forward and backward relationships between the source material and of the representations will allow ample notifications and reporting.

6.1.1.1 Use Case #1 - Sample Acquisition Language

- Learning Objects must be tagged according to the requirements in this document. All properties used MUST conform to the P2881 metadata standard. The contractor shall work with DoD Component to ensure all Learning Objects have a globally unique identifier that is also a URI. These URIs should include a "base" that is controlled by the DoD Component or is a persistent URL that resolves to a DoD Component controlled web domain.
- Unless a specific except is made by the DoD Component on a per Learning Object basis, every Learning Object shall be tagged with a title, description, and keywords. Each of these properties is unique in P2881. In the absence of these specific names of properties, substitutes may be used. The contractor shall work with DoD Component to determine if keywords are separate entities in a graph model/XML tags or can be considered a single string, and which solution is optimal for DoD Component learning environment.

- Do not design metadata around specific coding bindings (like XML), instead, define subject-predicate-object type relationships as seen in semantic web environments, and design toward each entity (subject or object) existing one time, and data pointing to that entity.
- For systems facilitating Learning Object search, discovery, acquisition and services, an algorithm shall be developed that meets a DoD Component's needs for optimized searches. Search results shall be constructed in a way that is meaningful to the user and empowers them to make a choice based on available metadata. Systems should take as many steps as securely possible to connect the user to the Learning Object (e.g., for download or content registration).
- Systems shall enable a UI that will allow the user to obtain all relevant metadata fields (P2881 and extensions) such that they can make an informed choice.
    - System shall provide controls for the user and use contextual information to determine if a user is searching for an available learning opportunity (instantiation) vs. a static resource (learning resource)
- If supported and/or desired by the DoD Component, Learning Objects shall be classified in accordance with a common catalog of subject areas made available by the DoD Component and captured in the "subject" (or equivalent) property. This catalog MAY include a Competency Framework for reference to determine the "subject" property values such that they are properly populated.
- If supported and/or desired by the DoD Component, Learning Objects shall be tagged to specific audiences provided by the DoD Component. Contractor shall work with DoD Component to determine if a classification of people or a generic description of whom the Learning Object is intended to serve is more appropriate.
- If supported and/or desired by the DoD Component, Learning Objects shall be tagged to specific geographical or regional context that is required for intended use of that Learning Object. DoD Component shall determine whether the Contractor or DoD Component is more qualified to provide this context. The Contractor shall work with DoD Component to determine if freeform expression of these contexts, or an integration with another service that adequately defines context, is more appropriate.
- Unless a specific exception is made by the DoD Component on a per Learning Object basis, every Learning Object shall be tagged with a language property. This language property shall be populated with values from ISO standards as referenced in the P2881 Learning Metadata standard.
- For each Learning Object, it shall be determined whether it is intended to be a static asset, a strategic learning component, or a deployed learning instance that requires resourcing (e.g., instructors, seat licenses) and the "scope" property (or equivalent) is populated with the corresponding restricted vocabulary term. This requirement is non-negotiable for compliance. If it is determined that a Learning Object is of more than one scope, it SHOULD be created as two distinct Learning Objects, one of each scope. For systems facilitating Learning Object search, discovery, acquisition and services, Contractor shall work with DoD Component to determine the impact on UI/UX based on scope type and user intentions/role. For almost all use cases, users should not see results from multiple scopes in the same search (e.g. they are looking for content for re-use, content for deployment, or a learning opportunity and not multiple of these at the same time).

- Unless a specific exception is made by the DoD Component on a per Learning Object basis, every Learning Object shall be tagged with a “learningObjectType” property (or equivalent). There are very few exceptions that would allow a Learning Object to be completely typeless. Contractor shall work with DoD Components to apply properties to the specific types of Learning Object in accordance with DoD Component requirements that are not part of the P2881 base model as represented in this document. Whenever possible, P2881 application profiles should be used for the corresponding type when populating additional metadata properties. In absence of profiles, DoD Component(s) should establish properties that are important as requirements (which essentially becomes a profile).
- If done in accordance with the P2881 standard, Learning Objects that use additional properties should not be penalized or considered non-conformant. Extensions should be realized through use of Learning Object types whenever possible.
- If supported and/or desired by the DoD Component, Learning Objects shall be tagged to specific competencies provided by the DoD Component. DoD Components should provide a competency framework/mapping to Contractor. A competency must be uniquely defined. A competency should use a URI as a unique identifier. A competency should have a representation that is obtained through resolution of that URI. That representation is beyond the scope of this standard’s guidance. Contractors should work closely with DoD Components to actualize competency-based alignment from resources to competencies to fit the DoD Component strategy. Learning Objects shall use both the “teaches” and “assesses” properties, and adequately populate those properties in accordance with alignment to which competencies are taught/assessed by the Learning Object. The same competencies are often taught and assessed using the same Learning Object.
- If supported and/or desired by the DoD Component, Learning Objects shall be tagged to in accordance with availability restrictions of DoD Component Systems as imposed upon those Learning Objects. Learning Objects that are considered not available (no permission to access) by the implementing system shall use the “availability State” (or equivalent) property.
- If supported and/or desired by the DoD Component, Learning Objects shall be tagged to in accordance with individual or role-based access of DoD Component Systems as imposed upon those Learning Objects. DoD Components shall provide specific integration points or system roles (providing a directory of individuals is not recommended) to the Contractor. The Contractor shall populate the “availabilityTo” property in accordance with DoD Component requirements and DoD security measures.
- For both of the previous properties that controlled availability and for systems facilitating Learning Object search, discovery, acquisition and services, the Contractor shall work with DoD Component to determine if the system permissions are used to populate the metadata, whether the metadata is used to inform the system permissions, or if consistency is met through another means.
- Unless a specific exception is made by the DoD Component on a per Learning Object basis, every Learning Object shall be tagged with properties that indicate the “previous revision”, if applicable. Similarly, Learning Objects that have been versioned/revised shall have metadata revisited to populate the “next reversion” (now that it is known). Contractors and DoD Components shall agree upon, and document, conditions for what a revision is defined as. For, systems facilitating Learning

Object search, discovery, acquisition and services, contractor shall work with the DoD Component to determine if the value of this property does rely on either a LCMS capability to populate it on publication or not.   The values of these properties should be the identifier of the referenced Learning Object. Systems are highly encouraged to implement the ability for the URI of metadata of the Learning Object to report/be subscribed to and provide adequate support.

- Unless a specific exception is made by the DoD Component on a per Learning Object basis, every Learning Object that is a derivation or has derivations that come from it shall be tagged with properties that indicate where it was derived from, if applicable. Similarly, Learning Objects that have been derivations shall have metadata revisited to populate which Learning Objects they were derived to (now that it is known). Contractors and DoD Components shall agree upon, and document, conditions for what a derivation is defined as. DoD Components should determine processes by which other DoD Components can share back derivations from their Learning Objects. DoD Components acquiring shared Learning Objects and then making their own modifications should consider it a derivation. For systems facilitating Learning Object search, discovery, acquisition and services, contractor shall work with the DoD Component to determine if the value of this property does rely on either a LCMS capability to populate it on publication or not.   The values of derivation properties should be the identifier of the referenced Learning Object. Systems are highly encouraged to implement the ability for the URI of metadata of the Learning Object to report/be subscribed to and provide adequate support.
- Unless a specific exception is made by the DoD Component on a per Learning Object basis, every Learning Object that has different representations shall be tagged with properties that indicate its original pre-representation/publication, if applicable. Similarly, Learning Objects that have been newly represented/published shall have metadata that point back to Objects from they originated. Not all DoD Components will have Learning Objects that have a single representation that then becomes multiple. Contractors and DoD Components shall agree upon, and document, conditions for representations and, how they relate to different published formats. For systems facilitating Learning Object search, discovery, acquisition and services, contractor shall work with the DoD Component to determine if the value of this property does rely on either a LCMS capability to populate it on publication or not.   The values of representation properties should be the identifier of the referenced Learning Object. Systems are highly encouraged to implement the ability for the URI of metadata of the Learning Object to report/be subscribed to and provide adequate support.

6.1.1.2 Use Case #1 - Sample Evaluation Criteria

- Evaluation criteria for individual tagging of Learning Objects should simply be a checklist of the if/then style bullets in Section 6.1.1.1. As the end “product” is either a metadata record or a Learning Object in a graph with all corresponding properties mapped, this becomes simply a yes/no evaluation for each property that is desired by the DoD Component.
- Some of the properties in the P2881 are mandatory or have explicit requirements for exceptions. It is recommended that DoD Components take these seriously and heavily penalize non-compliance.
- Extensibility is key for metadata. The more features and flexibility a tool has in creating / graphing additional properties, particularly from other existing metadata standards, and in supporting multiple Learning Object “types” (as application profiles), the better.

6.2 Related Policies and References

With the emergence of TLA Specifications and Standards, most related policies and references will be historical. These historical documents are valuable as they provide the context of what the old paradigm was and how different the new one is. The P2881 standard is still in draft as of July 2022, so the public reaction, adoption, lessons learned, and thus documentation will all be sparse. Metadata standards that influenced and that are referenced by P2881 are listed below. The Enterprise Course Catalog (ECC) effort is one that seeks to align content repositories across the DoD to this emerging standard.

- DoDI 1322.26 - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132226_dodi_2017.pdf?ver=2017-10-05-073235-400
- DoDI 1322.26 Reference - https://adlnet.gov/policy/fungible/
- DoDI 8320.02 - https://irp.fas.org/doddir/dod/i8320_02.pdf
- ADL Initiative P2881 Article - https://adlnet.gov/news/2021/05/28/P2881-and-the-Harmonization-of-Learning-Metadata/
- IEEE P2881 Page - https://standards.ieee.org/ieee/2881/10248/
- IEEE Learning Object Metadata - https://standards.ieee.org/ieee/1484.12.1/7699/
- Learning Resource Metadata Initiative (LRMI) - https://www.dublincore.org/about/lrmi/
- Dublin Core Metadata Initiative (DCMI) - https://www.dublincore.org/about/
- ADL Initiative 's Enterprise Course Catalog Page - https://adlnet.gov/projects/ecc/
- MIL-HDBK – 29612 Parts 1-5 - No links provided. Only historical value.
- Shareable Content Object Reference Model (SCORM) - https://adlnet.gov/projects/scorm/ (Multiple versions – these SCORM documents define the legacy approach to metadata in great technical detail)
  - SCORM 1.2 - https://adlnet.gov/assets/uploads/SCORM_1_2_pdf.zip
  - SCORM 2004 3rd Edition - https://adlnet.gov/assets/uploads/SCORM.2004.3ED.DocSuite.zip
  - SCORM 2004 4th Edition - https://adlnet.gov/assets/uploads/SCORM_2004_4ED_v1_1_Doc_Suite.zip

6.3 Recommended Best Practices

- Determine a DoD Component strategy for creating identifiers. This will allow the effective creation of metadata and linking between versions and across derivative works and publications.
- Some properties, if not used, leave the intended meaning ambiguous. DoD Components should determine vocabularies for some properties, such as audience, such that it is understood by both humans and machines what is meant by different values.
- When choosing how to handle "instances" of a particular Learning Object, consider creating a "representation" relationship between, for example, a course and a course instance. An alternative would be to have a "master" course instance that all other course instances are representations of. The point is to have a single point of update, such that if the underlying course were changed, course instances may also change. This would depend on the nature of

the update, whether those would propagate by rule to current instances, and if the course instance needed modification from the original course (as a learning resource).

- If more detailed publication metadata is needed, it is recommended that the DoD Component document this use case well and share it with the rest of the DoD Community.

6.4 Pitfalls to Avoid

- Never populate a metadata property simply to put something in the property. While lack of data is back, "junk data" is worse. This data is anything supplied to simply pass a technology requirement and has no value added.

6.5 Cybersecurity

Metadata in the P2881 standard doesn't necessitate any additional risks as the standard is only a data model. Effective data management policies should be followed, and processes executed regardless of the data. As P2881 describes learning activities and not individuals, there should not be any Personally Identifiable Information associated with metadata. However, some learning activities could be classified to a higher security level, so data associated with the learning activities should also be considered sensitive and potentially need to have restricted access.

Depending on the implementation of any metadata standard, whether it is through traditional metadata records or through semantic web technology like graphs, there will be technical safeguarding that needs to take place. Those recommendations are beyond the scope of this document.

7.0 Conclusion / Future versions

By leveraging completed acquisitions, sharing language and best practices, and both successes and failures, DoD capabilities will thrive as TLA standards are adopted and those products and services acquired through acquisition processes. This guidance is written in accordance with the DoDI 1322.26 as of 1 July 2022, and all referenced standards and profiles of those standards in their current forms and with current best practices. As standards mature, more best practices are defined, and additional successful acquisitions can be analyzed to produce more successful acquisition language, this document will be updated.