Expand All

1. Overview

Originally published in 2006 and revised in 2017, the Department of Defense Instruction (DoDI) 1322.26 ("Distributed Learning") establishes policy, responsibilities, and requirements for developing, managing, providing, and evaluating distributed learning for the Department of Defense (DoD) military and civilian personnel. It also addresses distributed learning modernization and charters the Defense ADL Advisory Committee (DADLAC) as the advisory body for DoD-wide distributed learning.

DoDI 1322.26 formally assigns responsibility to the Advanced Distributed Learning (ADL) Initiative and the DADLAC for maintaining the Instruction's References. These References define the most current technical requirements and best practices for distributed learning across the DoD. DoD Components are encouraged to refer to these References on a regular basis.

The ADL Initiative and the DADLAC update these References on a recurring basis to reflect current information or updates to referenced standards, specifications, conformance testing requirements, acquisition requirements, implementation requirements, or other distributed learning topic areas. Thus, these References change on a routine basis due to DoD evolving needs and technological advancements---too frequent to include in the base Instruction content outlined in the DoDI 1322.26 .

Contents of this Instruction support the DoD Data Strategy (DoD, 2020) and enable the DoD's distributed learning community to become an integrated, data-centric organization using data to improve the efficiency of how DoD personnel are trained and educated. This Instruction leverages specifications, standards, best practices, and industry guidance to make data visible, accessible, understandable, linked, trustworthy, interoperable, and secure.

The transition of the ADL Initiative to the Defense Human Resources Activity (DHRA) shifts responsibilities as defined in Section 2 of the DoDI to DHRA. This document addresses this change when referencing authority, direction, and organizational placement of the ADL Initiative under the Office of the Under Secretary of Defense (Personnel and Readiness) OUSD (P&R). The ADL Initiative roles and responsibilities do not change as part of this transition.

2. Technical Specifications and Standards

Distributed learning technical specifications and standards are published documentation of rules and guidelines designed to facilitate learning technology products, services, and data interoperability. These standards are referenced in Section 3 of DoDI 1322.26. They are community-driven, which enables interoperability across connected defense systems, networks, and organizations using consistent Information Technology (IT) protocols able to be universally adopted to share and interpret learner data. adopted to share and interpret learner data.

These references establish a comprehensive framework of policies, specifications, business rules, and standards essential for the effective operation of an enterprise-level learning ecosystem. Developed by Standards Development Organizations (SDOs), these standards focus on creating, publishing, or disseminating technical standards tailored to specific industries or fields. By adopting standards crafted by SDOs, DoD Components can rely on a credible source of information, the robust enforcement of those standards, and their recognition within

both professional and legal contexts. Notably, the Institute of Electrical and Electronics Engineers (IEEE), a prominent authority in standard development, formalizes these standards and enables the DoD to structure the necessary learning-related data, facilitating lifelong learning and promoting defense-wide interoperability.

The data standards defined within DoDI 1322.26 and these References are accessible in the DoD Information Technology Standards Registry (DISR). This online repository of IT standards facilitates the integration of distributed learning systems within the Global Information Grid (GIG). Standards added to the DISR are reviewed regularly for currency by DoD working groups, and usage of these standards by different DoD programs is documented in the registry.

2.1 Data Standards Usage and the DISR

"DoD organizations shall acquire and implement DL tools and technologies adhering to the specifications and standards described in this section."DoDI 1322.26 applies to any DoD IT network, information system, software, and service supporting any type of training, education, professional development, or career-field management functions within DoDDoD Components (e.g., accredited DoD academic institutions) may use additional specifications and standards as needed to improve functionality within their learning environment or to facilitate interoperability among non-DoD partners.

2.1.1 IEEE 9274.1.1 Experience API (xAPI)

The xAPI standard lays the foundation for the interoperable exchange of learning experince data for different types of learning activities. xAPI is both a learning technology standard and a web-service specification requiring a web-services application programming interface (API) for describing, recording, and sharing individual or team performance across digital learning systems. The xAPI standard requires from the server side, the use of a Learning Record Store (LRS). The LRS allows xAPI data to be shared with other systems requiring access to this data. Generation of xAPI statement is possible without an LRS. An LRS is necessary to capture and record xAPI data as a Learning Record Consumer (LRC). Additional information and access to the standard are available on the ADL Initiative's GitHub site.

2.1.2 IEEE 9274.2.1 Standard for JavaScript Object Notation for Linked Data (JSON-LD) for Application Profiles of Learner Experience Data

Also known as an **xAPI Profile**, is an emerging standard currently working through the IEEE standards development process. An xAPI Profile is a collection of xAPI Statement templates and patterns guiding the implementation of xAPI for specific media types, platforms, or training domains. Each xAPI Statement has at least one statement template describing when it will be used and what data is required to be conformant to a given xAPI Profile. Patterns define the relationship between xAPI Statements are also included in an xAPI Profile (e.g., a common sequencing of statements after a, successful or unsuccessful activity, is completed). A complete list of known xAPI Profiles can be accessed from the xAPI Profile Server . This standard serves as the template for the creation of xAPI Profiles. Additional information about the emerging standard is available on the ADL Initiative's GitHub site.

2.1.3 cmi5 (IEEE 9274.3.1)

The cmi5 specification builds on an xAPI Profile to enable all Sharable Content Object Reference Model (SCORM®) functionality using the xAPI standard. The cmi5 specification effectively replaces SCORM as the de facto standard used to deliver online courses and traditional computer-based training. Products supporting cmi5 also support xAPI. Additional information and resources are available at the cmi5 Project on GitHub. The cmi5 is now an IEEE draft standard and is expected to become an IEEE Open Standard in 2025.

2.1.4 IEEE 1484.20.3 Competency Data Standards: Sharable Competency Definitions (SCD)

is an standard that defineing a data model for describing, referencing, and sharing competencies, primarily in the context of online and distributed learning. Competencies are the data structure for describing the knowledge, skills, abilities, tasks, other behaviors, and/or assessment rubrics associated with the different jobs, work roles, and manpower requirements for meeting operational objectives. This standard formally describes the key characteristics of a competency, the relationship to other competencies within a competency framework, and assessment criteria for demonstrating proficiency (e.g., Outcome-Based). The SCD standard enables interoperability across DoD learning systems, human capital management systems, and other DoD functional areas using competency information. Competencies are described using linked data, which facilitates semantic interoperability among the vocabularies used to define each competency.

2.1.5 Credential Transparency Description Language (CTDL)

CTDL is a vocabulary of terms used to create assertions about a credential and its relationships to jobs, roles, career pathways, competencies, other credentials, etc. These terms refer to properties, classes, concept schemes, and/or data types and enable rich descriptions of credential-related resources, including credentialing organizations and subclasses of credentials such as degrees, certificates, certifications, and digital badges.

2.1.6 The Sharable Content Object Reference Model (SCORM)

SCORM is a legacy collection of standards that enables self-paced, asynchronous distributed learning delivered through a web browser. cmi5, as a preferred alternative using xAPI, has modern data storage and retrieval mechanisms and is more secure, interoperable, and flexible

2.2 Total Learning Architecture (TLA)

"The standards referenced within this document were created to maximize the capabilities across the DoD learning ecosystem. The capabilities desired for a DoD learning ecosystem come not from individual components or databases, but from the enterprise-level collection, dissemination, and analysis of data that support human capital accession, education, training. The Total Learning Architecture (TLA) defines 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 ecosystem. Within this ecosystem, multiple services and

learning opportunities (of various modalities and points of delivery) can be managed in an integrated, interoperable “plug and play” environment."

2.2.1 TLA Maturity Levels

TLA Maturity occurs by acquisition, use, and integration of specific systems and conformance to standards that are relevant to those systems or web services. The following levels of TLA Maturity contain corresponding following systems/services. Implied components that are not systems are shown in parenthesis only. TLA Maturity levels for each of the systems and services, as well as an overall way to “score” TLA Maturity, are listed in subsequent sections. Note: A Learning Content Management System (LCMS) is considered a Learning Management System (LMS) for the purposes of LMS requirements in this document.

Level 1:

- Learning Record store (LRS)
- Learning Management System (LMS)
- Analytics Dashboard
- (Courses)
- (Data Integration)

Level 2:

- Learning Record Store (LRS)
- Learning Management System (LMS)
- Analytics Dashboard
- Course Catalog
- (Courses)
- (Data Integration)

Level 3:

- Learning Record Store (LRS)
- Learning Management System (LMS)
- Analytics Dashboard
- Course Catalog
    - Uses the ECC
- Competency Registry
- Experience Index
- (Courses)
- (Data Integration)

Level 4:

- Learning Record Store (LRS)
- Learning Management System (LMS)

- Analytics Dashboard
- Course Catalog
    - Uses ECC
- Competency Registry
    - Uses the ECCR
- Experience Index
- (Courses)
- (Data Integration)

Level 5:

- Learning Record Store (LMS)
- Learning Management Systems (LMS)
- Analytics Dashboard
- Course Catalog
    - Uses the ECC
- Competency Registry
    - Uses ECC
- Experience Index
- Learner Profile
    - Uses ELRR
- Manpower and Personal Systems
- (Courses)
- (Data Integration)

2.2.2 List of TLA Technologies and Required Standards

The following TLA Maturity components are mapped to their corresponding standard and the means by which that standard is used. Sub-bullets denote which of the corresponding rubrics in Section 2.2.3 to use. Standards typically include a data model for structuring information and corresponding systems for data exchange. For the TLA Enterprise systems, standards compliance and TLA maturity scoring is accomplished on the data or resource components (italicized) and not actual systems or services.

- Learning Record Store (LRS)
    - Experience API (xAPI) sending/receiving
- Learning Management System (LMS)
    - xAPI structuring
    - cmi5 processing
- Analytics Dashcoard

    - xAPI receiving/processing
- (Courses)
    - xAPI structuring
    - cmi5 structuring
    - Learning Metadata Terms, P2881 (LMT) structuring (if level 2 or higher)
    - Shareable Competency Definitions (SCD) structuring (if level 3 or higher)
- Course Catalog Courses Ready
    - LMT structuring
- Competency Registry Competency Ready
    - SCD structuring
- Experience Index
    - xAPI structuring
- *Learner Profile Ready*
    - Enterprise Learner Record, P2997 (ELR) structuring
- Manpower and Personnel Systems
    - No standards at the time of this publication

2.2.3 Rubrics for Standards Levels

Shown below are the TLA standards with accompanying rubrics. The rubric used scores on a 1-5 scale with a description of how to achieve the score. Not all rubrics have five points, so the same criteria can be applied to multiple levels. In this case, the highest value may be chosen. As LMT processing, SCD processing, and ELR processing are not clearly defined at this time (there are not system-level requirements other than "handling" the conformant data), they will not be covered below. The capabilities of their corresponding systems, the ECC, ECCR, and ELRR, are continuously revised due to new requirements.

- **xAPI stucturing**

1. Use a proprietary, non-xAPI format
2. Some education and training activities capture learner performance data in xAPI format.
3. All education and training activities capture learner performance data in xAPI format.
4. All education and training activities capture learner performance data in xAPI format including use of UTC timestamps and generated Statement guides kept track of organizationally and properly.
5. All education and training activities capture learner performance data in xAPI format including use of UTC timestamps and generated Statement guides kept track of organizationally and properly. In addition, all activities have solid canonical metadata.

- **xAPI sending/receiving/processing**

1. No learner data is captured in a common LRS.
2. Some learner data is captured in a conformant and common LRS or set of LRSs.

3. Some learner data is captured in a conformant and common LRS or set of LRSs.
4. All learner data is captured in a conformant and common LRS or set of LRSs.
5. All learner data is captured in a conformant and common LRS or set of LRSs.

- cmi5 structuring

1. No xAPI profiles are required.
2. cmi5 is used for all tracked education and training session-based activities. (launch, initialize, terminate)
3. In addition to #2, some xAPI profile properties ensure data aligns with statement templates.
4. In addition to #2, some complete xAPI profiles and some additional xAPI profile properties ensure data aligns with statement templates.

- cmi5 processing

1. LMS doesn't use xAPI or cmi5.
2. LMS generates xAPI Statements from courses (cmi5 or otherwise) using cmi5 conformant data.
3. LMS is fully compliant with cmi5 and passes the Test Suite.
4. LMS is fully compliant with cmi5, passes the Test Suite, and allows dynamic use of table of contents, metadata from the course structure format, and other cmi5 best practices.
5. LMS is fully compliant with cmi5, passes the Test Suite, and allows dynamic use of table of contents, metadata from the course structure format, allows simple sequencing through the protocols in the cmi5 specification, and other cmi5 best practices.

- P2881 structuring

1. Activities are not tagged with any metadata.
2. Metadata records or entries into a system use LRMI metadata elements only.
3. Metadata records or entries into a system use LMT for Learning Resources only, except those which have to specifically reference other Learning Resources or Learning Events.
4. Metadata records or entries into a system use LMT for Learning Resources and Learning Events and use all properties correctly, unless a property is determined to provide no value. The lifecycle management properties cannot be determined to provide no value.
5. Metadata records or entries into a system use LMT for Learning Resources and Learning Events and use all properties correctly, unless a property is determined to provide no value. The lifecycle management properties cannot be determined to provide no value. In addition, at least one LMT profile is used and, if applicable, other extensions to LMT are used.

- SCD structuring

1. Competency definitions are not systematically defined or represented.
2. Some competency definitions are systematically defined (consistently follow a template) but may not be complete (not all data required by the template).
3. All competency definitions are systematically defined (consistently follow a template) and are complete (all data required by the template).
4. All competency definitions are in conformance with the SCD standard.
5. All competency definitions are in conformance with the SCD standard, align to Learning Resources, and have a defined rubric.

- P2997 structuring

1. Individual learner record is not systematically defined or represented.
2. Individual learner record includes data from all course completions.
3. Individual learner record includes data from all course completions, competencies, and learner preferences.
4. Individual learner record includes data from all course completions, competencies (both internally and externally to their organization), credentials, and leaner preferences.
5. Individual learner record includes data from external organizationally relevant HRs system; includes all relevant data on learner preferences/history, job requirements, learning activity, and all competency and credential data.

2.2.4 Data Integration:

Data integration is a major factor in scoring the TLA Maturity. Individual implementations of the systems are important, but so is data flowing across those systems and for higher TLA Maturity Levels, into the DoD as an Enterprise. The following rubric can be used to create an overall percentage score of the data integration:

- Begin with 100%
- Does the data go to Enterprise systems? If not, subtract up to 50% depending on the impact. (Not subtracted for levels where Enterprise systems are not present, but could be additive)
- Does data come back from each of the components? If not, subtract up to 10%, depending on the impact.
- Is the end data accessible by the end user? This is typically through dashboards, which are part of every maturity level. If not, subtract up to 40%.

2.2.5 TLA Score Calculator

To calculate a TLA score, use the following rubric.

- Declare a TLA Maturity Level (e.g., Level 1).
- Score each system/component against the standard(s)(e.g., LMS to xAPI structuring and cmi5 processing, LRS to Experience API (xAPI). sending/receiving, and Analytics Dashboard to xAPI receiving/processing)
- Each system must be at least level 2 to achieve any score.
- Average the component scores.
- Your max score is structured as “1””hyphen””that score”.
- An ideal max score is 1-5.0 for TLA Maturity Level 1, 5-5.0 for TLA Maturity Level 5.
- Calculate the connectivity score as a percentage multiplier for the second score as shown in Section 2.2.4 (e.g., if the connectivity score was 50%, then a TLA Maturity Level 1-5.0 would become 1-2.5)
- This is the final calculation of the TLA maturity score.

3. Acquisition Guidelines

DoD organizations shall follow this Instruction when acquiring distributed learning technology, courseware, and

other instructional content. This Instruction outlines specific requirements for systems and content, and these requirements shall be used whenever applicable. The specifications and standards referenced by this Instruction do not replace the primary requirements of an acquisition for specified product capabilities. Rather, this guidance supplements existing requirements to facilitate interoperability across tools and technologies that this Instruction applies.

Rare exemptions MAY exist where standards are already established for specific communities within DoD. DoD partnerships with non-DoD entities may also create situations where this Instruction cannot be fully implemented. In these cases, efforts shall be made to follow the Instruction **as closely** as possible.

3.1 Information Technology Systems Acquisition

This Instruction applies to the acquisition of Learning Management Systems (LMSs), Learning Content Management Systems (LCMSs), Student Information Systems (SISs), Learning Record Stores (LRSs), Competency Management Systems (CMSs), and other IT systems,such as those described in Section 2.2 used to manage the delivery of training and education content to DoD learners.

When acquiring a new DoD distributed learning system or updating an existing capability, DoD Components shall evaluate the acquisition of different tools, technologies, and systems or training and education programs using the following considerations to determine how this instruction applies.

- **Standards Compliance:** DoD Components shall develop or acquire distributed learning systems supporting the latest versions and editions of the specifications and standards defined in this Instruction to maximize interoperability. Compliance shall be aided, whenever possible, with the use of Conformance Testing software.
- **Data Interoperability:** DoD Components shall acquire distributed learning systems enableing the portability of data to other systems, such as those supporting human resources, student information management, and training management. Additionally, adherence to the xAPI standard shall be referenced throughout the acquisition process for any type of training and education system. If xAPI adherence cannot be met, the rationale for not utilizing the xAPI standard shall be provided. These include Requests for Information, Sources Sought Notifications, Statements of Work, and other types of requests for solutions.
- **Training:** DoD Components shall include a requirement to provide comprehensive training as part of any IT related acquisition. Training shall advance users' knowledge and skill sets on the use and application of the IT asset (e.g., if an LMS is acquired, training shall be provided to teach each group of users how to successfully use the LMS to meet their responsibilities). Component organizations shall determine the best format and source for training. A Continuing Education Unit (CEU) program for such training is recommended.
- **LRS Integration and Authentication:** This instruction does not define how an LRS is integrated into another IT system. An LRS may be included as part of a single product or may be deployed separately as a separate capability. However, stored data must be sharable and cannot be trapped in the data system. While this document describes the LRS capability using language describing a single system (e.g., "an LRS"), it is likely that multiple LRSs are used to filter, sort, and redirect data. The entire capability is still referred to as "LRS".

3.2 Learning Content Acquisition

The DoD acquires distributed learning content, often in the form of courseware, in support of its training and education programs. The ability of DoD Components to acquire source files and other software components for each acquisition in accordance with DoDI 5000.87, dated 2 October 2020, is critical to the reuse, repurpose, and reference of the distributed learning content.

DoD Components shall consider the following before acquiring new distributed learning content:

- **Standards Compliance:** DoD Components shall develop or acquire distributed learning content supporting the latest versions and editions of existing distributed learning specifications and standards described in this Instruction to maximize interoperability. Instructional content shall work with acquired IT systems to generate xAPI Statements for each learner. xAPI Profiles shall guide the requirements for how xAPI conformance is met within each media type used for instructional purposes. Compliance shall be aided, whenever possible, with the use of Conformance Testing software.
- **Data Interoperability:** DoD Components shall acquire distributed learning content using the specifications and standards outlined in this Instruction. Both xAPI and cmi5 shall be prioritized throughout the acquisition process for any distributed learning content (e.g., courseware and ancillary content).
    - The selection and use of xAPI Profiles should be included as requirements within the acquisition of new instructional content and specifically as part of the instructional design process. xAPI Profiles will be determined by the instructional domain, media types used, and other business rules within the DoD Component.
    - DoD Components should mandate all newly acquired or newly contracted online courseware to adhere to the cmi5 specification.
    - Failure to adequately address data interoperability will lead to content that cannot be re-used and learner data that is not interoperable.
    - If cmi5 and xAPI cannot be used, then new SCORM content may be part of training hosted on an LMS in accordance with Section 3.3.4.
    - Section 2.2 and Section 4-6.

3.3 Acquisition and Migration Strategy

When legacy (i.e., non-cmi5 compliant) courseware is updated, DoD Components shall start migrating away from SCORM-enabled courseware towards the cmi5 specification and the xAPI standard. The cmi5 specification facilitates the migration from LMS-centric (e.g., browser-based) courseware toward a distributed learning ecosystem delivering a diverse blend of learning opportunities across a range of federated platforms. cmi5 and xAPI address many of the technology problems that SCORM presents (e.g., not allowing content to be referenced externally).

The cmi5 specification defines a set of rules for how online courses are imported, launched, and tracked using an LMS and xAPI. The xAPI standard is used as the communication and data layer, and a cmi5-based implementation of xAPI implements controlled vocabularies, which are required for interoperability between LMSs and LMS-like systems. To support cmi5 acquisition, open-source tools and, including a Test Suite, and templates are available at the following link: https://github.com/adlnet/CATAPULT.

Identifying a candidate for acquisition shall include prioritization for those products that can demonstrate conformance to the standard. When available, the use of Conformance Test Suites shall be used to provide evidence of conformance of that product. At the time of this instruction, there are Conformance Test Suites for

both xAPI and cmi5(self-install). Adopter Registries of conformant products should be used to identify acquisition candidates, but responsibility of validation of conformance is still the requirement of the DoD Component. The ADL Conformant LRS site does include evidence of conformance to be included on the list. The cmi5 Adopter site has no validation of the claims made by those products.

Incrementally, DoD Components shall transition to using the cmi5 specification and the xAPI standard according to the following prioritized list of options in the following paragraphs: DoD Components shall:

- **Option 1:** Acquire and maintain a cmi5 conformant LMS and an xAPI conformant LRS.
- **Option 2:** If Option 1 is not possible, DoD Components should maintain their SCORM conformant LMS and use with an xAPI conformant LRS.
- **Option 3:** If a SCORM conformant LMS is not possible, then the DoD Component should acquire and maintain a standalone xAPI conformant LRS.
    - **NOTE:** It is possible to leverage an LMS in a manner that is not deploying learning or training content, e.g., for training event administration or other data recording. In these cases, xAPI is recommended to track events, but the SCORM requirement is waived.

If the above options are not possible, DoD Components may continue to use only their SCORM conformant LMS. Without an LRS capability, the ability to share learner data across systems will be severely compromised, undermining DoD modernization efforts. SCORM content (packages) impedes artificial intelligence (AI) functionality and interoperability, and additionally compromises DoD computing performance, productivity, and data science transformation efforts. While SCORM provides system interoperability, the inability to access data and the paradigm of an inflexible metadata "record" severely hinder modernization.

If DoD Components do not have a supporting system, both LMS-like and performance data should be continuously evolving toward use of xAPI and cmi5. Particularly for Options 2 and 3, the data should be modeled as cmi5 data until a suitable system is available.

The following sections outline the above options in greater detail.

3.3.1 Option 1: Acquire and maintain a cmi5 conformant LMS and an xAPI conformant LRS

The best option for xAPI migration is to leverage cmi5, which requires the use of both an LMS and an LRS.

- The LMS shall meet all requirements as tested by the cmi5 Test Suite . This conformance requires creating a testing script by the vendor of that LMS product. The LMS vendor should provide this script to the DoD Component making the acquisition for verification of the requirements.
- The cmi5 specification contains a vocabulary model and xAPI Statement patterns that are encapsulated as an xAPI Profile. (See cmi5 section in this document for more information about this specification).
- Beyond the xAPI standard, the cmi5 specification defines specific interoperability rules within an LMS for content launch, authentication, session management, reporting, and course structure definition. This is necessary because while the xAPI standard defines communication between a learning experience and an LRS, it does not define how online courses are structured or the communication between the learning content and the system hosting that content.
- To use a cmi5-enabled LMS, a LRS is needed, which may be standalone or integrated into the LMS platform. The preferred solution is a cmi5 LMS that can connect to any LRS. The LRS should conform to

the Quartz version of the cmi5 specification in addition to the requirements that it is an xAPI conformant LRS.

  - xAPI Statements should NOT be communicated to the LRS using **Basic Authentication** directly from a web browser. This method is not secure for the DoD. Data privacy and security should be implemented adhering to the organization's policy, environment, and security level.
  - LRS credentials and the xAPI payload should not be accessible by learners.

- The LRS shall conform to the ADL Initiative's LRS Conformance Test Suite for xAPI version 2.0 (IEEE 9274.1.1) or xAPI version 1.0.3.
- The LRS shall support authentication using the DoD's Identity, Credentialing, and Access Management (ICAM) https://dodcio.defense.gov/Library policies.

3.3.2 Option 2: Maintain a SCORM-conformant LMS with an xAPI LRS

An existing LMS solution may be integrated to work with a standalone LRS. This solution enables the LMS to collect traditional progress and completion data using the SCORM standard but also allows the LRS using the xAPI standard to replicate and augment SCORM data with additional learner performance data. The rationale for replicating SCORM into xAPI is to facilitate improved analytical insights across DoD functional areas.

The use of a SCORM LMS with the xAPI LRS has the following requirements:

- The LRS shall conform to the ADL Initiative's LRS Conformance Test Suite for xAPI version 2.0 (IEEE 9274.1.1) or xAPI version 1.0.3.
- xAPI 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.
- When considering integration with an LMS or any other system, the LRS cannot simply trust the other system and must take measures to ensure data integrity by preventing spoofing or implementing a direct pipeline accepting unauthorized users to send data to the LRS or send data that is not about the appropriate Actor.
- The LRS shall have the ability to send and receive data to/from other LRS implementations. The xAPI data will be accessible by other DoD systems.
- The LRS shall support authentication using the DoD's Identity, Credentialing, and Access Management (ICAM) https://dodcio.defense.gov/Library policies.
- Any xAPI Statements used to replicate SCORM should be modeled after those used in cmi5. Some SCORM equivalents require the use of "cmi5 allowed" statements and would model as extensions if implemented.
- The LMS shall conform to all mandatory requirements for a supported version of SCORM (supported versions are SCORM 1.2, SCORM 3rd Edition, and SCORM 2004 4th Edition).

3.3.3 Option 3: Acquire and maintain a standalone xAPI LRS

If deviation from this Instruction is required because the use of cmi5 is not an option and SCORM LMS support is

not possible, DoD Components shall implement an xAPI-conformant LRS capability. Use of xAPI Profiles is highly encouraged. The xAPI standard does not include any authentication protocols to connect learners to content. Choosing this option will require additional software to effectively connect the learner to the content.

This solution has the following requirements:

- xAPI 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.

The standalone xAPI LRS has the following requirements:

- The LRS shall conform to the ADL Initiative's LRS Conformance Test Suite for xAPI version 2.0 (IEEE 9274.1.1) or xAPI version 1.0.3.
- The LRS shall have the ability to send and receive data to/from other LRS implementations. The xAPI data will be accessible by other DoD systems.
- The LRS shall support authentication using the DoD's Identity, Credentialing, and Access Management (ICAM) https://dodcio.defense.gov/Library policies.
- If considering integration with an LMS or any other system, the LRS cannot simply trust the other system and must take measures to ensure data integrity by preventing spoofing or implementing a direct pipeline accepting unauthorized users to send data to the LRS or send data that is not about the appropriate Actor.
- Any xAPI Statements used to replicate SCORM should be modeled after those used in cmi5. An example would be tracking the completion of a performance task on a standalone application that does not report to an LMS.

3.3.4 Exception: Maintain and use only a SCORM conformant LMS

Maintaining a SCORM conformant LMS is an acceptable option for existing systems that are unable to undertake migration efforts in the direction of cmi5, but is seen as an exception to data standards compliance. Legacy SCORM instructional content is still widely used across the DoD. Any DoD Component that does not have a SCORM conformant LMS (and has not met any of the options described above) shall immediately upgrade its LMS to be compliant with this Instruction. New acquisition efforts should not use SCORM.

SCORM conformance testing tools are not actively supported by the ADL Initiative. The ADL Initiative does offer hosting and troubleshooting of these tools to DoD Components, but no software maintenance or updates will be provided. Legacy tools and samples are available on the ADL Initiative website https://adlnet.gov/projects/scorm/ .

The use of a SCORM LMS has the following requirement:

- Conforms to all mandatory requirements for a supported version of SCORM (supported versions are SCORM 1.2 and SCORM 2004 (3rd & 4th Edition).

3.4 Identity, Credentialing, Access, and Management

When acquiring software, DoD Components shall follow DoD's policy for ICAM. The DoD ICAM Strategy

enhances DoD's ability to track, manage, and optimize lifelong learning. ICAM enables DoD organizations to link an individual's DoD ID to training and education records that are created and stored across various DoD schools and training sites.

Identity information for the DoD community is managed through the Defense Manpower Data Center (DMDC). It operates the Defense Enrollment Eligibility Reporting System (DEERS), which includes the Person Data Repository (PDR). PDR is the primary identity attribute repository and to-be standard as IEEE for Public Key Infrastructure (PKI) certificates for all DoD persons, including military, civilian, and contractors. The DoD Common Access Card (CAC) combines PKI with a physical ID card, and CACs have become the cornerstone of trust for identifying and authorizing access to DoD personnel.

Pursuant to **Homeland Security Presidential Directive 12** (HSPD-12), the DoD has recently transitioned from using CACs with DoD-specific credentials to using CACs with Personal Identity Verification (PIV) credentials. This maintains DoD's legacy authentication mechanisms while also allowing the Department to use products designed to read the more modern, HSPD-12 compliant PKI credentials.

Formerly, the DoD ID number was synonymous with the Electronic Interchange Personal Identifier (EDIPI), a unique 10-digit number assigned to each person registered in DEERS. Now, with the shift to PIV credentials, the DoD ID number has become a 16-digit number, better supporting joint interoperability across government.

The following requirements of this guidance can assist in maintaining the security and privacy of learner data:

- No Personal Identifiable Information (PII) should be included in the Actor property of any xAPI Statement.
- When using digital learning content, tools, systems, or services that generate xAPI data, 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.

The DoD should consider syncing up and using a common homepage, such as **https://www.defense.gov/** as this would allow a DoD ID to propagate across all Services and DoD activities for easier data aggregation. Those without DoD ID would simply need congruence with an approach that would keep their ID unique across the DoD. If the common homepage is not used, the "homepage" property value chosen by the DoD Component SHALL be under DoD control.

3.4.1 Personally Identifiable Information in Data

The expanded use of the DoD ID Number has led to questions regarding its status as PII, which refers to information that can be used to distinguish or trace an individual's identity. The DoD ID Number falls into this category because it is a unique personal identifier and can be used to retrieve records about an individual. Presence or knowledge of an individual's DoD ID Number alone does not constitute any level of authority to act on that individual's behalf.

The DoD ID Number, by itself or with an associated name, shall be considered internal government operations-related PII. Since the loss, theft, or compromise of the DoD ID Number has a low risk for possible identity theft or fraud, a PII breach report will not be initiated unless the breach is associated with other PII elements, such as date of birth, birthplace, or mother's maiden name, which would normally require a report to be submitted. As detailed in **DoDI 1000.30** , "Reduction of Social Security Number (SSN) Use Within DoD", exposure of the DoD ID Number shall not be considered a breach when exposed as part of a DoD business function.

3.4.2 Ethical Principles in Artificial Intelligence (AI)

Ethical considerations for AI are a key element in a more reliable and safe operations under specific development and testing standards. Currently, there no formal verification processes for Machine Learning (ML) that exist today. As a result, DoD officially adopted five Ethical Principles for Artificial Intelligence (February 2020) along with an Executive Steering Group (DoD, 2020). The following are the five main ethical principles for AI capabilities according to the DoD AI Ethical Principles and the DoD Responsible Artificial Intelligence Strategy and Implementation Pathway (OUSD, 2023):

1. Responsible. Appropriate levels of judgment and care, and responsible for the development, deployment, and use of AI capabilities.
2. Equitable. Deliberate steps to minimize unintended bias in AI capabilities.
3. Traceable. Appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedures and documentation.
4. Reliable. Explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life cycles.
5. Governable. Capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems demonstrating unintended behavior.

Reference: Office of the Under Secretary of Defense for Policy (OUSD) (2023, January 25). DOD DIRECTIVE 3000.09, Autonomy in Weapon Systems. Retrieved from https://www.esd.whs.mil/DD/.

3.4.3 Zero Trust Architecture Guidance

When acquiring software, DoD Components shall follow DoD's Reference Zero Trust Architecture (ZTA). Zero Trust is the term for an evolving set of cybersecurity paradigms moving defenses from static, network-based perimeters to focus on users, assets, and resources.

The DoD's need to connect data across multiple networks, devices, software systems, and organizational boundaries requires a cybersecurity architecture. This architecture precludes default trust of any actor, system, network, or service operating outside or within the security perimeter using a data-centric approach to establish continual verification of each user, device, application, and transaction. This is especially important when considering the acquisition and implementation of new learning tools and technologies. DoD Components are encouraged to consider ZTA data management operations to improve how data is handled by its systems. The DoD CIO has a substantial amount of guidance relevant to this Instruction, including ZTA at https://dodcio.defense.gov/Library/ .

3.5 Section 508 Accessibility

DoD Components shall meet requirements included in DoD Manual 8400.01 (Accessibility of Information and Communications Technology). This set of requirements helps ensure new IT systems and instructional content meet or exceed requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C 794d). Section 508 requires agencies to ensure that individuals with disabilities have access to and use of information,

communication technologies, and data comparable to the access and use afforded to individuals without disabilities. Standards and methods for development and testing distributed learning systems for Section 508 compliance are available at Section 508.gov .

DoD Components shall thoroughly examine revised Section 508 compliance of any new distributed learning systems and its applications, including authoring tools. The revised Section 508 standards include usage of Web Content Accessibility Guidelines (WCAG) 2.0 and future versions. The Voluntary Product Accessibility Template, commonly referred to as VPAT, is one method for such examination. VPAT is a document used to evaluate how accessible an application is according to the revised Section 508 standards.

3.6 Adobe Flash®

The Adobe Flash plug-in was a browser-based technology commonly used to support web-based courseware and content development. Adobe ended support for Flash in 2020, and Internet browsers also ceased support for Flash that year. As a result, DoD Components:

- Shall not acquire any distributed learning content, tools, websites, or any other capability containing any Adobe Flash code of any version or derivative of Adobe Flash.
- Shall not update or modify any distributed learning content, tools, websites, or any other capability to a state containing Adobe Flash code such that an end user is allowed to execute that code. This includes non-Adobe Flash modifications leaving the content, etc., in a state of containing Adobe Flash.
- Shall carefully analyze the user interface and output of authoring tools, including web tools or plug-ins, currently in use for underlying Adobe Flash technology, and desist using tools found to contain or use any form of underlying Adobe Flash technology.
- Shall thoroughly examine the controls, interfaces, and capabilities of distributed learning systems for Adobe Flash use or reliance before acquiring them. Deprecation of Adobe Flash has rendered dependent features useless and creates security vulnerabilities within systems that use it.

3.7 Acquisition Language and Requirements

The ADL Initiative released version 1.1 of the TLA Standards Digital Learning Acquisition Techniques Report document to assist DoD acquisition personnel on integrating learning technology standards into their acquisition processes. This document shares established language that has been used in successful acquisitions for use across the DoD. The language in this document includes standards requirements referenced in the DoDI and in a DoD Component's past acquisitions of distributed learning technology. This guidance will be updated periodically as standards advance and as subsequent successful acquisitions are shared. This resource complements the DoDI by enabling acquisition personnel to utilize sample language by copying/pasting requirements aligning with the DoDI's overarching guidance into their acquisition proposals. It includes guidance on the implementation details of standards as well as draft profiles of some of those standards.

4. xAPI Implementation and Integration

The primary purpose of this section is to provide content developers with best practices, technical guidance, and standard requirements for implementing xAPI in DoD learning environments. This section assumes an understanding of the xAPI specification version 1.0.3 or the IEEE 9274.1.1 standard (xAPI 2.0), and the underlying

concepts explained within those standards. The guidance in this section is intended to serve as the baseline of minimum technical requirements for any learning content that is required to support xAPI.

4.1 xAPI Statement Requirements

The xAPI Statement Data Model provides content developers with the ability to represent learning experience and performance data in a structured manner. Statements are modeled using JSON Objects and are fundamentally expressed in the form "Actor, Verb, Object" or "A Person(s) did something." Statements also typically include additional information in the Result and Context Objects to add more meaning or details about the learning experience. A high-level diagram of the primary parts of the xAPI Statement Model is provided below.

Figure 1: High-level Parts of the xAPI Statement Data Model

Actor will represent the individual person (Actor) who performed the action (Verb) in a given Statement. The Actor in an xAPI Statement SHALL include the following:

- 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. If the Actor is a group of learners, set the ***actor.objectType*** property with the value set to "Group". If using a group, determine which practices are best for the use case as opposed to the rest of the Actor guidance below.
- Set the ***actor.account.homepage*** property with the value set to an organizationally appropriate and controlled URL.
- Set the ***actor.account.name*** property with the Electronic Data Interchange Personal Identifier or PIV associated with the user. (i.e., DoD ID).

Verbs convey the action that occurred in an xAPI Statement. The Verb in an xAPI Statement is represented in the past tense since the Statement is triggered immediately after a learning experience or event occurs.

- The Verb in an xAPI Statement SHALL include the following:
  - 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.
- The Language Map for the Verb display SHALL include a display string in English with the language code of "en".

Objects of an xAPI Statement define the subject or object that was acted on. The Object can be an Activity, Agent/Group, Sub statement, or Statement Reference. By default, Objects will be an Activity unless otherwise specified in a particular xAPI Profile. Objects are defined by their Activity Type. Some examples of Activity Types include the following: course, lesson, video, question, page, file, link, etc.

- The Activity Object in an xAPI Statement SHALL include the following:
  - The ***object.id*** shall reference a unique Activity ID used by the learning activity generating the xAPI statement, or as a reference to a different activity.
  - Set the ***object.definition.name*** to the language map value representing the official name or title of the Activity.
  - Set the ***object.definition.description*** to the text value representing a short description of the

Activity.

- Set the *object.definition.type* to the identifier associated with the relevant Activity Type.

- The Activity Object in an xAPI Statement SHALL NOT:
  - Use multiple Activity IDs to represent the same Object.
  - Reuse the same ID to represent different activities.

4.2 Activity ID Requirements

These requirements ensure that there is no possibility of accidentally creating and using the same Activity IDs for different activities.

The Activity ID for an Object in an xAPI Statement includes the following requirements:

1. The Activity ID is based on a valid internationalized resource identifier (IRI) starting with https://.
2. The Activity ID SHALL NOT include any spaces.
3. An Activity ID SHALL NOT end with a trailing slash "/" unless the slash is required to resolve to the URL of an external resource.
4. 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.
5. 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.
6. The Activity ID SHALL NOT include any URL-encoded characters unless it's required to resolve to the URL of an external resource.
7. 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.
8. Do NOT use multiple Activity IDs to represent the same Object or reuse the same ID to represent different activities.
9. Create a unique Activity ID according to the recommended scheme and example table below. Note: The Uniform Resource Identifier (URI) in this example is structured around The Naval Education and Training Command, the hosting organization of the activity. Different DoD Components would use URIs within their control.
10. Content developers SHALL maintain an inventory list of Activity IDs used for each project in 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 document that should be updated and shared with all relevant stakeholders.

Table 2: Activity ID Examples

Context: The **Context** property of an xAPI Statement contains additional information related to a learning experience. It provides a place to add some contextual information to a Statement. It could store information such as the instructor for an experience, if this experience happened as part of a team-based Activity, or how an experience fits into some broader activity. Please see the general xAPI Statement requirements for examples of these objects and their properties in the sections below.

Context Activities: Many statements do not just involve one (Object) Activity that is the focus but relate to other contextually relevant Activities. The ***context.ContextActivities*** property allows for these related Activities to be represented in a structured manner. Valid context types include “parent”, “grouping”, “category”, and “other”.

Context Activities Category: When an xAPI Statement is composed, the ID of the xAPI Profile Activity it conforms to SHALL be declared (using the id property and other optional properties) in the category array as part of the ***context.ContextActivities*** property. Additional Profile Activity IDs for each xAPI Profile SHALL also be declared in the category array for each xAPI Profile that is used in an xAPI Statement (e.g., https://w3id.org/xapi/cmi5/context/categories/cmi5).

Context Registration: The ***context.registration*** property is used to identify multiple xAPI Statements that are all part of a particular user’s experience throughout interacting with that activity. It should be managed differently than the concept of an attempt (e.g., a user may fail one attempt on an assessment and re-take the assessment as a part of another attempt). The value of the Registration property SHALL be a UUID and should persist throughout all Statements during the registration and likely across all attempts. There is no expectation that completing an Activity ends a registration.

Context Extensions: The values of the ***context.extension*** property can be any JSON name/value pair or a JSON Object. Extensions in the "context" property provide context to the core experience, while those in the "result" property provide elements related to some outcome. Within Activities, extensions provide additional information helping to define an Activity within some custom application or Community of Practice.

Context Platform: The ***context.platform property*** property is used to specify the platform (e.g., software or hardware) used while the Actor experienced the content. xAPI Statements are required to include the ***context.platform property*** property if the value is known. The value of the ***context.platform property*** property SHALL be a text string and will vary depending upon the xAPI Profile used.

Timestamps: The timestamp property is used to provide the time when a learning experience occurred. All Statements SHALL include a timestamp. A timestamp SHALL be formatted according to the RFC 33393. This format uses the Gregorian Calendar and Coordinated Universal Time (UTC). The “Z” suffix denotes a UTC offset of 00:00, which is known as Zulu time. For example: 2020-04-30T23:20:50Z. This example represents 20 minutes and 50 seconds after the 23rd hour of April 30th, 2020, in UTC. In contrast, 2020-06-27T12:55:32-0500 represents 55 minutes and 32 seconds after the 12th hour of June 27th, 2020 in the Eastern Time Zone (GMT-5).

- The timestamp in an xAPI Statement SHALL include the following:
  - The timestamp must represent the date/time of when the event occurred. Not a future time.
  - The timestamp shall be formatted according to RFC 3339 (ISO 8601 normal).
  - The timestamp shall be formatted using the Gregorian Calendar with a time zone offset specified.

4.3. Authoring xAPI Enabled Resources

There are additional best practices to follow for authoring tools, xAPI Profiles, and data design. DoD organizations should use cmi5- or xAPI-supported authoring tools for the creation of xAPI content. If using non-cmi5 xAPI Profiles, the authoring tool should support xAPI version 1.0.3 or later. Context agents were introduced in xAPI 2.0, so version 2.0 should be used if DoD organizations want to take advantage of that addition. The xAPI Statements generated by an authoring tool should be compared to available xAPI Profiles to ensure interoperability. Since xAPI enables many more opportunities for the expression and tracking of learning

experiences, reporting on xAPI data generated by distributed learning content can be complicated. When working with xAPI content, the following processes shall be followed:

1. When mapping learner interactions to xAPI Statements, the xAPI implementation (e.g., Verbs, Activity Types, concepts, patterns) should leverage a suitable xAPI Profile. Existing xAPI Profiles shall be used rather than creating a new xAPI Profile performing the same function. The ADL Initiative maintains a listing of these profiles deemed to be suitable for DoD usage.
2. When mapping learner interactions to xAPI Statements in the context of an LMS or LMS-like activity, first use those in cmi5 to align with the typical Statements found in tracking a learner's activity in the LMS distributed learning model.
3. If the intended function of an xAPI Verb is slightly different from an existing verb, or additional information is needed, use the xAPI properties such as **context**, **result**, or **extensions** to add this data to the Statement.
4. Where applicable, the use of multiple xAPI Profiles is encouraged. Examples include using cmi5 for course-based content and the Video Profile for any sort of media (audio/video). A complete list of known xAPI Profiles can be accessed from the **xAPI Profile Server** which can be seen on **Github.**
5. If existing xAPI Profiles do not meet requirements, then consider creating a new xAPI Profile using the xAPI **Profile Server Authoring Guide** located on the ADL Initiative website. All new xAPI Profiles shall be shared with the ADL Initiative such that they may be put online for discovery at a single point of reference.
6. Profile authors SHALL follow Internationalized Resource Identifier (IRI) design best practices. The following IRI pattern should be adopted by anyone creating new concepts for a profile: https://w3id.org/xapi/ [profile name] / [concept type] / [concept]. Profile 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.
7. xAPI Profiles should include information about the profile, such as the name, description, authoring organization or person, and the publication date/time.
8. Those already familiar with xAPI and implementing cmi5 should adhere to the following conformance guidance when designing learning content:
    - Use of specific verbs and results as documented in the cmi5 specification.
    - Use of cmi5-defined Verbs once per user per activity.
    - Use "tagging" statements with contextActivity as defined in the cmi5 specification.

4.4. cmi5 Usage

The cmi5 specification/draft IEEE standard (IEEE 9274.3.1) is the initial step forward for all LMS and non-LMS based content. It enables the packaging and delivery of distributed learning resources that sit inside an LMS, elsewhere within a browser environment, and even outside of a web browser (e.g., mobile apps, simulation content).

- The cmi5 specification has a clear advantage over SCORM, specifically relating to the authenticity of learner data. The use of timestamps and incorporation of the SCORM *cmi.interactions* model into xAPI provides an advantage in data integrity. It also allows the LMS to implement its own sequencing model while providing structure for those LMSs wishing to obtain to it from an external source, such as the original course author. The cmi5 specification enables LMS to migrate away from using SCORM, which

includes control of the learning environment by an LMS Administrator, which was sometimes automated in SCORM solutions but is an integral part of typical learner management.

- cmi5 "courses" (collections of granular/modular content put together in a Course Structure Format) allow an LMS administrator to edit learner or course details like mastery score if they would like to do so. In this regard, a cmi5 course author is providing recommendations to an LMS administrator that can be used or not upon the importing of that course. Similarly, the completion criteria for a course can be altered by the LMS administrator. This means that cmi5 courses do not need to be "re-authored" to simply change behaviors, but it does mean more intervention and handling will be needed by an LMS administrator.
- When launching content from a cmi5 LMS, the LMS shall be configured to perform the launch using the cmi5 launch protocol. In this case, the content does not need to form the xAPI Actor or hardcode the LRS credentials. This information is provided to the content as part of the launch. The content shall use the information provided via launch over any locally configured information.
- For content that is not web-based or situations where there is a need to have the Actor's identity anonymized, DoD Components should use LRS Endpoints and localized authentication requirements for launching, testing, and deploying xAPI.
- To enable the migration from SCORM content, which allows for internal behaviors relative to learner performance and to course structure, cmi5 MAY be extended to support the use cases of "testing out" and defining "pre-requisites".
- Open source tools and templates are available at the following link: https://github.com/adlnet/CATAPULT/ These are free templates but are intended to be starting points for DoD Components. The ADL Initiative developed a cmi5 plug-in for the Moodle LMS that can allow Moodle as a course/activity type in that platform. DoD components may develop alternate solutions and should do so as requirements necessitate. This Instruction provides the following recommendations for the use of these resources for cmi5 acquisition. DoD Components pursuing acquisition of cmi5 conformant systems or content SHALL:
    - Leverage cmi5 course templates. Modifications may be made to templates to add additional features or to support additional use cases. The use of standardized templates will reduce the time to create new cmi5 content and repurpose existing content. Content may also be modified before or after application of the templates.
    - Use the cmi5 Test Suite to verify that cmi5 content, LMSs, and/or authoring tools (producing cmi5 content) are conformant to the cmi5 specification.
    - 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.

5. Activity and Resource Management

To support the DoDI requirement to "make existing DL assets, content, and other reusable resources visible and accessible to other DoD Components", this section describes how DoD Components can effectively manage learning activities, content, and other resources throughout their product lifecycle. Activity and resource management guidelines enable content sharing and discovery through the use of metadata. Learning activity metadata is structured data describing different types of learning activities and the resources each activity requires to be successfully delivered to a learner.

The Learning Metadata Terms (LMT) draft standard, which has been approved by the IEEE P2881 Working Group, was designed to meet use cases of increasing visibility and accessibility of reusable resources. Metadata creation should conform to this draft standard and should be done on all Learning Resources and Learning Events. Details of those requirements are listed below.

5.1. Metadata Sharing and Content Discovery

In the context of distributed learning, metadata provides information about learning content (e.g., author, file size, subject, title, duration). Many types of metadata exist, including descriptive, structural, administrative, reference, and statistical metadata. Metadata describes Learning Resources at any level of granularity and Learning Events, which are opportunities that are contextualized by time and place. Each type has varying characteristics, including those of assets, content, learning resources, and learning activities. Learning metadata can be used to facilitate defense-wide search and discovery of each resource and event, enables artificial intelligence and machine learning, and provides improved insight into the lifecycle of DoD learning resources.

DoD Components should adhere to the following metadata guidance for their learning content as well as other applicable training and education materials:

- All learning resources and where possible, events (e.g., courses, activities, course offerings) should be tagged with metadata. The emerging LMT standard should be used when creating learning metadata tags for distributed learning resources and events. The IEEE P2881 standard references and therefore reuses many existing metadata standards and is extensible, so using it should align to any standards-based current practice. An example of an application profile of course metadata is included in the TLA Acquisition Guidance referenced in Section 3.7.
- Develop a strategy allowing all learning activity metadata to be accessible and interoperable across the DoD. Such solutions allow for storage and retrieval of Learning Resources, or the metadata records themselves. Solutions should also provide the ability to update the metadata at a single point (described in the URI recommendations outlined above in section 4.3. Authoring xAPI Enabled Resources - item 6).
- Learning metadata should include data describing the alignment of Learning Objects to the different educational frameworks used by an organization, such as competency frameworks (e.g., Sharable Competency Definitions), Enabling and Terminal Learning Objectives (ELOs and TLOs), Skill matrices; Training & Evaluation Outlines; or other established frameworks). Alignment metadata should delineate whether the Learning Object teaches, assesses, or both.
- Consider a metadata strategy delineating each Learning resource (or events) as having specific properties for the diverse types of learning activities used within an organization to educate and train. Learning activity types might include courses, webinars, on-the-job training, virtual classrooms, lectures, or any xAPI activity type. Learning activity types may be embodied within an LMT application profile. Each profile should include only fields specific to that learning activity type (e.g., technical information, contextual data, pointers to other data types collected in an activity). Constraints on metadata properties (e.g., allowed terms, value ranges, etc.) should also be documented in metadata application profiles.
- Metadata may include additional technical information, contextual data about the delivery of an instance of that Learning resource or event, and pointers to other types of learner data collected within a particular activity.
- A learning event shall be used to uniquely identify multiple instances of a learning activity/resource. Learning events may describe multiple delivery schedules for the same learning activity, but as uniquely identified objects. A learning instantiation should consider how logistics such as seats, instructors, or

time slots are managed in their data strategy.

- Metadata about Learning events should have a location (physical or virtual), start/end dates, and a schedule.
- Metadata should include data about the current version of a Learning Object and should reference one or more active versions of it.
- Metadata should describe the lineage and provenance of different learning activities, establishing revisions, derivations, and representations of those objects using a matrix of Activity IDs and cross-reference each other using the LMT standard.
- Use IRIs (or URIs) for all identifiers, such that they can be transitioned to a semantic web or DoD schema server in the future. Whenever possible, store relevant information at the resolution point of the IRI. This information should include, at minimum, a resource description and location.
- Do not design metadata around specific coding bindings (like XML). DoD Components should define metadata using subject-predicate-object type relationships as seen in semantic web environments using the Resource Description Framework Model and Syntax Specification . Each entity should exist once, and all data should point to that entity.
- Avoid use of complex activity types and "nested" data elements within metadata (such as defining an author of a course and then putting author name and contact information inside the author "tag"). Instead, data about that person should be captured and then the person is linked to by the author tag. This way, other metadata properties and records can refer to the same person and humans/machines/AI will know they are the same person.

6. Competency-Based Learning

Competence is a set of demonstrable behaviors, characteristics, and skills enabling the effective performance of a job. Competency-Based Learning (CBL), also called Outcome-Based Learning, is a model of learning design focusing on the mastery of competencies required for a job. Each competency, when defined as data, is broken down into the specific knowledge, skills, abilities, or other behaviors (KSAOs) required to perform a job at different levels of proficiency. To demonstrate competence, an individual or team must be able to demonstrate outcomes by performing certain tasks or skills at a required level of proficiency.

Competency definitions describe the specific details, contexts, related standards, mastery levels, and credentials required to successfully demonstrate the KSAOs necessary to successfully perform a job in an operational environment. Competency definitions include identified learning resources or events satisfying or contribute to satisfaction of that competency. Competency frameworks are used to define the relationships between established competencies. The frameworks are hierarchical in nature, but a single competency may be used across numerous frameworks (e.g., jobs, occupations), so data connections among competencies are required to express all relationships they have.

DoD Components SHALL use IEEE 1484.20.3 SCD to describe their competencies, competency frameworks, and assessment criteria as soon as they are mature enough to be defined by any standard.

6.1 Implementing Competencies

To enable a competency-based / outcome-based learning strategy, DoD Components shall begin to define competency definitions, competency associations, and competency frameworks as described in IEEE 1484.20.3

–Shareable Competency Definitions. The granular unit, often referred to as a "competency", is a competency definition in SCD. These are referred to as "competencies" throughout this Reference.

Based on industry best practices and the IEEE 1484.20.3 standard, DoD Components should:

- Implement a strategy allowing all competencies to be accessible and interoperable across DoD Components. Competency Definitions and Competency Frameworks should be referenceable within a Competency Registry allowing for storage and retrieval of competencies and their associated Frameworks. Competencies and their Frameworks should also support versioning and alignment of similar competencies. Competency Registries should be able to update competencies and their frameworks at a single, referenceable, IRI (following the IRI recommendations outlined below).
- Document local competencies in a manner that adequately describes each competency and meets the following requirements:
    - Competency Definitions shall include unique IDs in the form of an IRI. Each competency should also have a text representation that is definitive and descriptive.
    - Competency Definitions shall include a human-readable expression describing a competency (e.g., Operation of a Gear Stick and Clutch in a Commercial Vehicle)
    - Competency Definitions shall include a narrative in plain language describing and contextualizes the competency (e.g., This competency relates to the operation of a commercial vehicle that a civilian would normally operate. Certain vehicles have a manual transmission, which requires the ability to manually control a gear stick with precision and timing as the vehicle changes gears when moving between drive/neutral/park and when reaching certain speed thresholds.)
    - Competency Definitions shall include a name or label that would be viewed within a competency framework. (e.g., ManualTransmissionMastery)
- Competency Definitions and Competency Frameworks should support resource association describing relationships within the context of the competency framework and its ecosystem. Competency Frameworks can be created at multiple levels. An industry best practices guide for competency-based education has also been published by IEEE (1484.20.2) that should be used to inform DoD implementations.
- Relationships (expressions) between Competency Definitions should be described using an association property. The types of relationships should focus on both hierarchical (one member belongs to a larger group) and ordered (an intended pre-requisite exists) relationships. This overrides any generic notion of parent/child relationships of competencies; the design should be with intent. Examples would be a set of quiz questions making up an assessment (hierarchical) or a direct series of lessons building on the previous lesson making up a course (ordered).
- Use an association property to link to other relevant organizational Competency Frameworks, as applicable.
- Competency Definitions should include assessment rubrics to describe performance criteria for different proficiency levels within an individual competency where applicable, Assessment rubrics should separate one level of competence from another. Creation of rubrics is recommended. Levels may be designed using the rubric criterion if implemented within a rubric.
- When versioning competencies and Competency Frameworks, maintain the version history, including if a competency or competency framework was derived from a separate effort that is not considered a previous version.
- Consider using IEEE 1484.20.3 SCD extensions to describe relationships and metadata within competencies and competency frameworks using public schemas.

6.2 Credentials

To better align learner data with human capital management systems and software systems used across other DoD functional communities, DoD Components should start to define and document occupations/jobs, roles, tasks, learning opportunities, credentials, and assessment profiles in a digital representation. The preferred mechanism to do this is Credential Transparency Description Language (CTDL). The scope of the CTDL is restricted to a description of credentials offered and not the description of credentials awarded. In other words, awarding, appraising, or validating a credential, including the information about the person earning the credential and the issuing authority and the dates of associated events are not in scope of CTDL.

CTDL is used to align competencies and credentials with jobs, career milestones, and future opportunities when transitioning from DoD into the civilian sector.

CTDL relies on linked data to facilitate semantic interoperability as an approach to combining data about things from different sources, particularly among the vocabularies used to define credentials, competencies, jobs, tasks, etc.

The CTDL family of specifications is built on the principles of the Resource Description Framework (RDF) approach to describing resources. As such, CTDL allows for a linked data approach to combining information about resources from different sources, the use of CTDL with terms from other RDF specifications and expressing the relationship between terms in CTDL to similar terms in other specifications. In some cases, CTDL has been designed in the expectation that there will be future integration. In some cases, a standards development organization (e.g., IEEE) may overlap with CTDL. If a data conflict arises, choose the solution using the standards development organization.

The W3C Recommendation on Verifiable Credentials (W3C-VC) is complementary to CTDL in that the W3V VC data model allows the expression of the information needed to appraise and validate a credential held by an individual. The Recommendation also describes how such data can be made tamper-evident and can be shared within a distributed credentialing ecosystem. The terms in the data model alone do not allow for much information about the nature of the credential, which is deliberately left as broad as possible, however for those credentials relating to educational or occupational achievements CTDL can be used to fill in the details.

In the future, CTDL may include integration to other standards, such as IEEE's SCD and define pathways to competency frameworks. Currently, CTDL leverages its own rules that are specific to competencies and competency frameworks, but these are not recommended at this time.

If a DoD Component chooses to implement competency-based learning, SCD is still the preferred strategy. Should there be a conflict between details of SCD and CTDL, CTDL should not be used.

7. References

United States Department of Defense. (2020). Executive Summary: DoD Data Strategy - Unleashing Data to Advance the National Defense Strategy. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

DoDI 1322.26 DL Implementation References PDF

View the PDF