DoDI 1322.26 DL Implementation References

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 that uses 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 that can be universally adopted to share and interpret learner data.

These References define a set of policies, specifications, business rules, and standards which are necessary for the functioning of an enterprise-level learning environment. The standards are developed by Standards Development Organizations (SDO) that focus on developing, publishing, or disseminating technical standards to meet the needs of an industry or field. By using standards developed by SDOs, DoD Components can be assured of an authoritative source of information and legal enforcement of that standard. The Institute of Electrical and Electronics Engineers (IEEE), a leading developer of industry standards, formalizes these standards to organize the learning-related data required to support lifelong learning and enable defense-wide interoperability.

The data standards defined within DoDI 1322.26 and these References are accessible in the DoD Information Technology Standards Registry (DISR) (https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/). 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.

DoD organizations shall acquire and implement DL tools and technologies that adhere to the specifications and standards described in this section. DoDI 1322.26 applies to any DoD IT networks, information systems, software, and services that support any type of training, education, professional development, or career-field management functions within DoD. DoD 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 IEEE 9274.1.1 Experience API (xAPI): The xAPI standard lays the foundation for the interoperable exchange of learning data. xAPI is both a learning technology standard and a web-service specification that requires a web-services application programming interface (API) for describing, recording, and sharing individual or team performance across digital learning systems. The xAPI standard 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 this data. Additional information and access to the standard are available on the ADL Initiative's GitHub site (https://github.com/adlnet/xAPI-Spec/blob/master/xAPI-About.md#partone).

2.2 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**, this emerging standard is currently working through the IEEE standards development process. An xAPI Profile is a collection of xAPI Statement templates and patterns that guide the implementation of xAPI for specific media types, platforms, or training domains. Each xAPI Statement has a statement template that describes when it will be used and what data is required. Relationships between xAPI Statements are described using patterns. 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.

2.3 cmi5: 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 that fully support cmi5 also support xAPI. Additional information and resources are available at the cmi5 Project on GitHub.

2.4 IEEE 1484.20.3 Competency Data Standards: Sharable Competency Definitions (SCD) is an emerging standard that defines a data model for describing, referencing, and sharing competencies, primarily in the context of online and distributed learning. 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 that use competency information. Competencies are described using linked data, which facilitates semantic interoperability among the vocabularies used to define each competency.

2.5 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, other credentials, etc. These set of 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. (https://credreg.net/ctdl/handbook).

2.6 The Sharable Content Object Reference Model is a legacy collection of standards that enables self-paced, asynchronous distributed learning delivered through a web browser. xAPI has modern data storage and retrieval mechanisms and is more secure, interoperable, and flexible. Standards within SCORM were recently renewed by the IEEE in order to maintain SCORM as a standard to extend support while the DoD transitions to xAPI and cmi5. Additional information is available on the ADL Initiative website.

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.

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 reasonably 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 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 that support the latest versions and editions of the specifications and standards defined in this Instruction to maximize interoperability.
- **Data Interoperability:** DoD Components shall acquire distributed learning systems that enable the portability of data to other systems, such as those that support 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 adequate training as part of any training and education-related IT 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 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 that supports 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.
- **Data Interoperability:** DoD Components shall acquire distributed learning content that use 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 a 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 acquired 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, Option 4: Maintain and use a SCORM-compliant LMS.

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 environment that delivers a different blend of learning

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 templates are available at the following link: https://github.com/adlnet/CATAPULT.

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

The following section outlines the above options in greater detail.

3.3.1 Acquire and maintain a cmi5 conformant LMS and an xAPI conformant LRS

Option 1: 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 (https://github.com/AICC/cmi-5_Spec_Current/blob/quartz/cmi5_spec.md) of the cmi5 specification in addition to the requirements that   it 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 DoD. Data privacy and security should be implemented that adhere 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.
- The LRS shall support authentication using the DoD's Identity, Credentialing, and Access Management (ICAM) (https://dodcio.defense.gov/Library) policies.

3.3.2 Maintain a SCORM-conformant LMS with an xAPI LRS

Option 2: 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
- 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 that accepts 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.

- 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 Acquire and maintain a standalone xAPI LRS

Option 3: 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

- 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 that accepts 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 Maintain and use only a SCORM conformant LMS

Option 4: No new acquisition effort should use Option 4. Maintaining a SCORM conformant LMS is an acceptable option for existing systems that are unable to undertake migration efforts in the direction of cmi5. 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.

The SCORM standards were recently renewed through the IEEE Learning Technology Standards Committee to support continued use while the tools, technologies, and infrastructure are put in place to support widescale adoption of xAPI and the cmi5 specification (e.g., Conformance Testing).

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, SCORM 3rd Edition, and SCORM 2004 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 for Public Key Infrastructure (PKI) certificates for all DoD persons, including military, civilian, and contractors. DoD's 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), 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 that better supports 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.
- There is no specific recommendation on the "homepage" property other than making sure it is 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 a part of a DoD business function.

3.4.2 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 that move 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 that uses 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/.

3.5 508 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 508 compliance of any new distributed learning systems and its applications, including authoring tools. The revised 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 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 that contains 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 that contains Adobe Flash code such that an end user is allowed to execute that code. This includes non-Adobe Flash modifications that leave 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 1.0 of the Standards Acquisition Guidance 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 that align with the DoDI's overarching guidance into their acquisition proposals.

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 1.0.3 or the IEEE 9274.1 standard, 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.

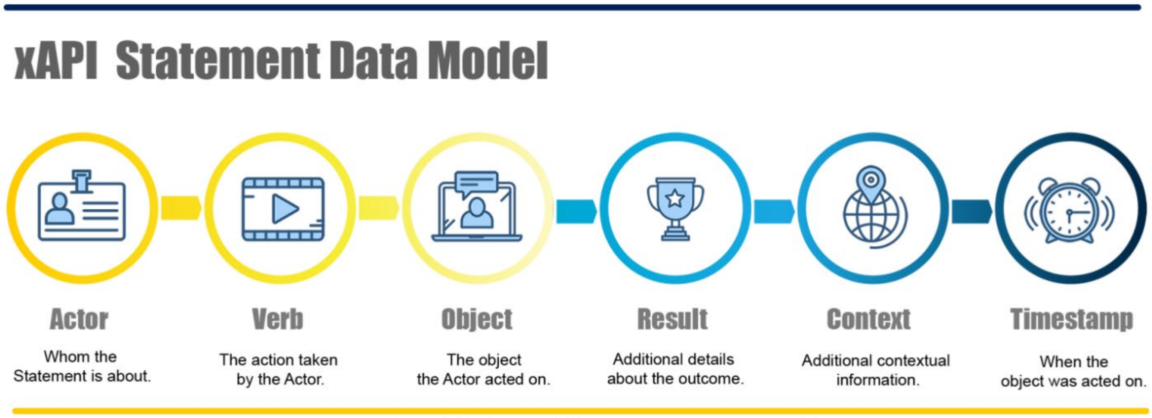

xAPI Statement Data Model
Actor
Whom the Statement is about.
Verb
The action taken by the Actor.
Object
The object the Actor acted on.
Result
Additional details about the outcome.
Context
Additional contextual information.
Timestamp
When the object was acted on.

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 that generates the xAPI statement, or as a reference to a different activity.
  - 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.

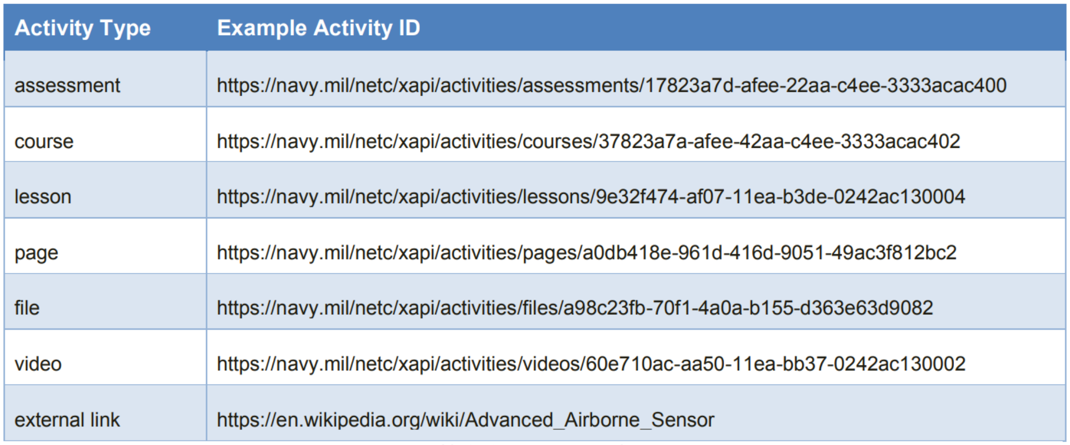
- The Activity Object in an xAPI Statement SHALL NOT:
  - Use multiple Activity IDs to represent the same Object.
  - Reuse the same ID to represent different activities.

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.



Activity Type	Example Activity ID
assessment	https://navy.mil/netc/xapi/activities/assessments/17823a7d-afee-22aa-c4ee-3333acac400
course	https://navy.mil/netc/xapi/activities/courses/37823a7a-afee-42aa-c4ee-3333acac402
lesson	https://navy.mil/netc/xapi/activities/lessons/9e32f474-af07-11ea-b3de-0242ac130004
page	https://navy.mil/netc/xapi/activities/pages/a0db418e-961d-416d-9051-49ac3f812bc2
file	https://navy.mil/netc/xapi/activities/files/a98c23fb-70f1-4a0a-b155-d363e63d9082
video	https://navy.mil/netc/xapi/activities/videos/60e710ac-aa50-11ea-bb37-0242ac130002
external link	https://en.wikipedia.org/wiki/Advanced_Airborne_Sensor

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 ***contex***t.***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 that helps define an Activity within some custom application or Community of Practice.

Context Platform: The ***context.platform*** 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 if the value is known. The value of the ***context.platform*** 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. 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 that performs 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.

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 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 detecting cheating through data manipulation. It also allows the LMS to implement its own sequencing model while providing structure for those LMSs that wish to obtain 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. 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 (that produce 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 that describes different types of learning activities and the resources each activity requires to be successfully delivered to a learner.

In a future update, further guidance will be provided to increase visibility and accessibility of reusable DoD resources by describing processes and infrastructure to follow for conformance to the shareability of resources. Data and system requirements already promote reusability, but specifically, to enable visibility and accessibility in the future, documentation (at this time of an unspecified format) of metadata is the only requirement for conformance.

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 Objects at any level of granularity. Learning Objects, a catch-all term, have 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, 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 (e.g., courses, activities, events) should be tagged with metadata. The emerging IEEE P2881 metadata standard should be used when creating learning activity metadata tags for distributed learning resources as it becomes available. The IEEE P2881 standard references and therefore reuses many existing metadata standards.

- Develop a strategy that allows all learning activity metadata to be accessible and interoperable across the DoD. Such solutions allow for storage and retrieval of Learning Objects 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 activity metadata should include data that describes 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 that delineates each Learning Object as having specific properties for the different 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 a P2881 application profile. Each P2881 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 Object, and pointers to other types of learner data collected within a particular activity.

- A learning instantiation shall be used to uniquely identify multiple instances of a learning activity/resource. Learning instantiations may describe multiple delivery schedules for the same learning activity, but as unique Learning Objects. A learning instantiation should consider how logistics such as seats, instructors, or time slots are managed in their data strategy.

- 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.

- 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”).

6. Competency-Based Learning

Competence is a set of demonstrable behaviors, characteristics, and skills that enable the efficient performance of a job. Competency-Based Learning (CBL), also called Outcome-Based Learning, is a model of learning design that focuses on the mastery of competencies required for a job. Each competency 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 (i.e., demonstrate) 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 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.

6.1 Implementing Competencies

To enable a competency-based / outcome-based learning strategy, DoD Components should begin to define competency definitions, competency associations, and competency frameworks as described in IEEE 1484.20.3 – SCD. 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 draft standard, DoD Components should:

- Implement a strategy that allows all competencies to be accessible and interoperable across DoD Components. Competency Definitions and Competency Frameworks should be referenceable within a Competency Registry that allows 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 that describes a competency (e.g., Operation of a Gear Stick and Clutch in a Commercial Vehicle)

    - Competency Definitions shall include a narrative in plain language that describes 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 that describe relationships within the context of the competency framework and its environment. 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 that build 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.

CTDL relies on linked data to facilitate semantic interoperability among the vocabularies used to define each credential. CTDL is used to align competencies and credentials with jobs, career milestones, and future opportunities when transitioning from DoD into the civilian sector.

> The CTDL family of specifications is built on the principles of the Resource Description Framework (RDF) approach to describing data. CTDL allows the use of terms from other RDF specifications when describing resources. 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 that uses the standards development organization.
>
> In the future, CTDL will 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