ADL Initiative • FY20 Broad Agency Announcement Topic

Accredited xAPI Learning Record Store (LRS)

Problem Statement. *The Experience Application Programming Interface (xAPI) specifies how data from learning activities are captured, stored, and retrieved. A Learning Record Store (LRS) is the implementation of the server-side requirements of the xAPI specification. To support the enterprise-wide adoption of xAPI across the Department of Defense (DoD), LRS solutions need to be accredited to run on DoD networks.*

Background: DoD Instruction 1322.26 recommends the xAPI data specification as the primary method for encoding and exchanging interoperable learner-performance data. In a federated system-of-systems, xAPI makes data from a diverse range of technologies interoperable across technical and organizational boundaries. The xAPI specification includes guidance for encoding learner data (xAPI statements) and for storing/retrieving data to/from an LRS. In 2015, the ADL Initiative released the xAPI LRS Conformance Test Suite, a web-service that helps DoD organizations validate whether new technologies they plan to acquire adhere to the xAPI specification.[1] In FY20, the ADL Initiative is funding an xAPI Profile Server, which will enhance the semantic interoperability of xAPI-enabled systems. The wide-ranging interoperability enabled by xAPI also presents a complex cybersecurity challenge. As a result, DoD has not accredited (to date) an xAPI LRS for operational unclassified networks.[2]

Outcomes: This effort will **demonstrate an accredited LRS collecting xAPI data** from two or more sources across an unclassified DoD network and then exchanging data between them; this reference implementation will help provide a baseline of cybersecurity management approaches for other DoD organizations. The ADL Initiative will provide a partner organization for the prototype testing, but offerors may suggest other testing venues. To perform this operational trial, the project will require successful completion of the DoD accreditation processes, and the performers are expected to deliver all **associated documentation**, including supplementary guidance to aid DoD stakeholders in completing similar cybersecurity accreditation processes. This documentation package must also conform with all necessary Security Technical Implementation Guides (STIGs). The ultimate goal is to support the development of xAPI as an approved transport protocol and to evaluate whether a type-accreditation or other enterprise-level approval for all of DoD is viable. As part of this process, performers should **advise the ADL Initiative** on best practices for cybersecurity accreditation of other xAPI-enabled systems and provide recommendations to make future xAPI system accreditation processes more cost and time efficient. Recommended revisions to the xAPI specification or its supplementary implementation guidance are encouraged as needed.

Note: Offerors should indicate their proficiency with DoD cybersecurity accreditation, DoD networks, and xAPI.

Summary of Major Objectives	Associated Deliverables
Conduct analysis, per RMF[3] and FISMA[4] guidance	System security plan
Author STIG	xAPI STIG
Secure necessary accreditations for demonstration	Accredited DoD cybersecurity package for IATT or IATO [5]
Demonstrate successful operational prototype	Documented transfer of xAPI data across DoD network
Author STIG testing guidance	Instructions for testing LRSs and verifying compliance
Author automated testing suite updates, per STIG	Directions for updating xAPI LRS Conformance Test Suite
Provide recommendations to DoD	Recommendations report and "How to" guides

[1] https://lrstest.adlnet.gov/

[2] See Hernandez et al. (2019). Cybersecurity Strategies for Accrediting Experience Application Programming Interface, I/ITSEC.

[3] The Risk Management Framework (RMF) standardizes processes for cybersecurity across the federal government

[4] The Federal Information Security Management Act (FISMA) provides additional guidance for DoD systems

[5] IATT = Interim Authority to Test; IATO = Interim Authority to Operate

For more information see: https://adlnet.gov/research-baa and FedBizOpps BAA #HQ0034-18-BAA-ADL