An Overview of the DoD's DevSecOps Reference Design and its Intersection with the Learning Technology Warehouse

Jason Weiss, DoD
Brent Smith, ADL Initiative (SETA)
Chad Udell, Float
ADL Initiative Webinar

November 17, 2021
Ability to Fight and Win is Software Dependent

- **New software = new capabilities**: Capabilities of weapons systems and other critical systems are defined by their software
- **Rapidly respond to emerging threats**: Response to emerging threats is increasingly determined by the time required to develop and deploy software to the field
- **Enable innovation**: Modern software practices are critical to effective use of new technologies: cloud computing, artificial intelligence, machine learning, robotics, internet of things
- **Challenge**: The current approach to software development is a leading source of risk to DoD: it takes too long, is too expensive, and exposes warfighters to unacceptable risk
- **Need to accelerate**: Improvements in how we acquire software are happening, but adoption has been limited

Software is a foundational component of the modern military
DevOps

A change in IT culture, focusing on **rapid IT service delivery** through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture), and it seeks to improve **collaboration between operations and development teams**. DevOps implementations utilize technology — especially **automation** tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective. *(Gartner IT Glossary)*

DevSecOps

The **integration of security** into emerging agile IT and DevOps development as **seamlessly and as transparently** as possible. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment. *(Gartner IT Glossary)*
DOD SOFTWARE MODERNIZATION

Resilient Software Capability at the Speed of Relevance

TECHNICAL ENABLERS

- Enterprise Services
- D3CEOps/Tooling
- DSECS/Cloud Environment
- Design Patterns
- Application Design Patterns
- Data Infrastructure Design Patterns
- Architecture Services
- Data & AI/ML
- Digital Engineering
- Spectrum
- Quantum
- 5G
- Blockchain
- IoT Sensors
- Quantum Computing
- Data & AI/ML
- Digital Engineering

PROCESS TRANSFORMATION

- Business Operations
  - Must enable "shared services economy" for reusable software within DoD
  - Must drive efficiencies and agility in developing requirements and budgeting for modern software
- Acquisition
  - Must adapt to the unique needs and faster pace of modern software development
  - Must establish a shared risk and common platform model between DoD and industry
- Cyber Survivability
  - Must automate cyber authorization to keep pace with software delivery
  - Must stay to the left of threats/incidents by continuously monitoring cyber operations and supply chain risk
- Testing
  - Must integrate testing processes in software pipelines
  - Must address software function and performance in meeting interoperability and operational test and evaluation criteria
- Business Operations
  - Must enable "shared services economy" for reusable software within DoD
  - Must drive efficiencies and agility in developing requirements and budgeting for modern software

OUTCOMES

- Faster Software to Mission Capabilities
- Greater Automation in Business Ops
- Strengthened Data Advantage
- Better Active Cyber Defense

Workforce

- Must evolve the workforce to address changes in process and technology triggered by modern software development
- Must drive toward a technology-literate workforce and advance technical competencies.
Role of the DevSecOps Software Factory
Zero Trust and Baked-in Cybersecurity

DoD Enterprise DevSecOps Reference Design:
CNCF Certified Kubernetes

- Sidecar Container Security Stack (SCSS)
- Service Mesh Mandate
- Locally Centralized Artifact Repository
- CNCF Certified Kubernetes (K8s)
- Cloud Native Access Point Utilization
DevSecOps Advances Cybersecurity

- Defensive Cyber Operations
- Continuous Monitoring
- Secure Software Supply Chain

Security  NOT MUTUALLY EXCLUSIVE!  Speed
Putting DoD's DevSecOps Reference Design into Practice

Brent Smith
RD&E Principal
ADL Initiative (SETA)
About the ADL Initiative

PROGRAM:
Advanced Distributed Learning (ADL)

DIRECTOR:
Sae Schatz, Ph.D. (CIV)

PURPOSE:
Facilitate interoperability and promote best practices for Distributed Learning (DL)...

DoDI 1322.26: “The ADL Initiative is the principal steward for researching and facilitating the implementation of DL standards, specifications, and emerging technologies for DoD Components.”
Agenda

1. Overview of Connected DLE Systems
2. DLE Software Factory (It’s not just Buzzword Bingo)
3. Moving Forward with the DLE FOC
4. Future Work
   - Conformance Testing
   - Standards Based
   - Learning Technology Warehouse
   - On-demand Accessibility
Centralized Event Streams / Decentralized Data Products
# TLA – Related Resources

<table>
<thead>
<tr>
<th>Type</th>
<th>Title</th>
<th>Year</th>
<th>Authors</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>Reimagine Education</td>
<td>2021</td>
<td>Schatz, S.</td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>Podcast</td>
<td>The Future Learning Ecosystem with Sae Schatz</td>
<td>2021</td>
<td>Schatz, S.</td>
<td>LeadingLearning.com</td>
</tr>
<tr>
<td>News</td>
<td>Building the Infrastructure for DoD Digital Learning Modernization</td>
<td>2020</td>
<td></td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>News</td>
<td>DoD Reform Effort Puts Digital Learning Systems at the Forefront</td>
<td>2020</td>
<td></td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>Webinar</td>
<td>ADL-DAU Sandbox: TLA and Competency-Based Learning Demonstration</td>
<td>2021</td>
<td></td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>Project</td>
<td>Total Learning Architecture</td>
<td>2021</td>
<td></td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>Publication</td>
<td>Total Learning Architecture: IDA Report</td>
<td>2020</td>
<td>Barr, A.; Fletcher, J.D.; Morrison, J.</td>
<td>ADLnet.gov</td>
</tr>
<tr>
<td>GitHub</td>
<td>ADL Initiative</td>
<td>2021</td>
<td></td>
<td>GitHub.com/adlnet</td>
</tr>
</tbody>
</table>
Enterprise Digital Learning Modernization (EDLM)

EDLM’s Goal: Acquire and deliver DoD digital learning more effectively and cost-efficiently. This requires improvements to (1) acquisition and sustainment processes and (2) modernization.

Why?

- $485M+ annual spend
- Personnel readiness
- Modernization

Realizes cost and time savings
Meets growing operational demands
Implements policy guidance
DoD Learning Enclave (DLE): Overview of Connected Systems

What systems can I run in the DLE?

DoD Owners

Iron Bank

Learning Technology Warehouse

Enclave 1
- Moodle
- LRS
- CaSS
- Learner Profile
- Local Catalog
- Other

Enclave 2
- SABA
- PQS
- Spotlite
- LRS
- CaSS
- Learner Profile
- Local Catalog
- Other

Enclave 3
- CSOD
- Qualtric
- Domino
- LRS
- CRMS
- Learner Profile
- Local Catalog
- Other

Enclave 4
- ADLS
- cmi5
- PtN
- LRS
- CompA
- Learner Profile
- Local Catalog
- Other

Enclave 5
- ALMS
- GoSkills
- Teams
- LRS
- CaSS
- Learner Profile
- Local Catalog
- Other

Enclave 6
- PeBL
- Moodle
- QMark
- LRS
- CaSS
- Learner Profile
- Local Catalog
- Other

DoD Owners
Mission Partner Confirmation of TLA Services

Linked Data
for Metadata definitions, Competencies, Credentials...

Linked Data Database

Enterprise Course Catalog
Experience Index
Kafka

Enterprise Learner Record Repository
Learner Records

Enterprise Competency Registry
Competency Frameworks

PBAC (Future)
KeyCloak
Digital Learning Web Portal

USASOC (Operational Testing)
Experience Index (XI)
Learner Profile
Competency Registry
Web Portal
Kafka
TLA Core
Moodle
PERLS
cmi5
Noisy LRSs

Operationalization & Test

NETC MNL
Army STEEL-R
DAU

Learning Technology Warehouse

Learning
Technology
Warehouses

1. Enterprise Course Catalog
2. Enterprise Learner Record Repository
3. Enterprise Competency Registry
4. Schema.mil
5. Learning Technology Warehouse

Noisy LRSs
DoD Learning Enclave (DLE): Systems

Enterprise Systems:

- Enterprise Course Catalog - Deloitte
- Enterprise Learner Record Repository - Deloitte
- Competency and Skills System - ADL
- Linked Data and Schema Server - Deloitte
- Learning Technology Warehouse – Float / PT

Learning Activities:

- TLA Core – ADL
- Moodle Course Management System – ADL
- PERLS Microlearning Platform – Float / PT
- Cmi5 Player – ADL
- LRS – ADL

External Systems:

- xAPI Profile Server
- LRS Conformance Test Suite
- Cmi5 Conformance Test Suite
- DataSim
Software Ecosystem
Multiple Innovation Hubs – One Platform

43 PMOs & PEOs Across Services
Ventures & Non-Traditional Start-ups
DoD-wide Enterprise Services
AF Ventures
Software Factories
Science & Technology
Defense Industrial Base
Other Agencies

Integrity - Service - Excellence
Understanding the DevSecOps Layers

- **Environment Agnostic**
  - Cloud One Preferred for unclassified (IL2, IL4, IL5)
  - Or SC2S/C2S/FENCES
  - Or on-premise/embedded systems/classified environments

- **Development Team**
  - Selects between approved K8S stacks
  - Selects tools from 172 approved containers or custom containers

- **Development Teams**
  - Can build software/microservices leveraging hardened containers
  - Brings baked-in security and Microservices architecture enablement

- **CNCF compliant Kubernetes (K8S)**
  - Includes Site Reliability Engineers (SREs) etc.

- **Infrastructure Layer**
  - Environment Agnostic

- **Platform Layer**
  - Continuous Integration / Continuous Delivery (CI/CD) Layer

- **Service Mesh Layer**

- **Application Layer**

- **You**

- **Cloud One**
  - Continuous Monitoring
  - Leverages the Sidecar Container Security Stack

- **Platform One**
DoD Learning Enclave (DLE): Major Tasks

• Onboarding
• Commit Source Code to Platform One GitLab Repo
• Integrate Source Code with Iron Bank Containers
• Container Hardening & Vulnerability Testing
• Refactoring to address any Identified Vulnerabilities
• Container Hardening Approval Process
• Certificate to Field
• Establish Dev and Test in IL2
• Establish Production Environment in IL4

Major Milestones:

• Onboarding
• IOC software integrated with Iron Bank Containers
• Validated Containers (GitLab CI Pipeline)
• Container Hardening Approval Process Submission
• Approved Certificate to Field
• Deployed Systems
## DLE IOC Implementation – POA&M

<table>
<thead>
<tr>
<th>DoD Shared Services for Learning Technology</th>
<th>O</th>
<th>N</th>
<th>D</th>
<th>J</th>
<th>F</th>
<th>M</th>
<th>A</th>
<th>M</th>
<th>J</th>
<th>J</th>
<th>A</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>End-user Learning Technologies (LOE1)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Learning Management System (Moodle)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Microlearning app (PERvasive Learning System)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• cmi5 Player (Added capability to LMS)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLA Core (Interoperable Data Services)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Total Learning Architecture Core (e.g., Kafka, Data)</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
<td>♦</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schema Server for Linked Data</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Learning Technology Warehouse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Course Catalog (LOE2)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ECC IOC application</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Learner Record Repository (LOE3)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Learning Record Store</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ELRR Prototype Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Competency and Skill System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DLE IOC CI/CD Milestones.** (♦ = other milestones, ◆ = Certificate to Field, ★ = Initial Use)
DLE FOC Considerations for Moving Forward

Defense-wide Reciprocity
• Collaboration with the Cloud Computing Program Office
• Collaboration with DoD CIO (e.g., ICAM, Zero Trust, DevSecOps Reference Design)
• Collaboration with DoD stakeholders – Integrated Program Team

Analysis of Alternatives
• Fast Track ATO, Traditional ATO, Continuous ATO?
• Cloud Agnostic Tools and CSP Native (e.g., Big Bang / DoD Cloud IaC, or a Collection of CI/CD pipelines?)
• What’s the best strategy moving forward for DoD?
• Lifecycle Costs / Configuration Control Board / Governance

Leveraging work done on the DLE IOC
• Lessons Learned / Best Practices using Party Bus tools, workflows, and methodologies
• Istio Service Mesh / Sidecar Container Security Stack
• Iron Bank is a Defense-wide resource
• Tailor the DevSecOps Pipeline based on DLE and Authorizing Official Requirements
• Creating a Culture – This isn’t about the Tech as much as its about the Mindset of our People
DLE FOC Implementation

Estimated Review & Remediation duration is 11-17 weeks

January

DoD Sponsor completes Initial Contact Forms. Meetings to review DLE requirements to determine best path to Provisional Authorization

February

Joint Validation Team: SCA, Sponsor, Analysts, CSP, 3PAO
Access to CSP Document repo, initial review of RAR, SSP, SSP Addendums, & documentation checklist, Review and approve SAP

Initial Contact Phase

DHRA Business Case Analysis

DLE Sponsor submits ICF to DISA

Onboarding Kickoff

DISA / DHRA holds process & requirements strategy meeting

April

DoD Review & Remediation 8-10 weeks

3PAO ASSESSMENT

SCA, JVT, and CSP review and approve SAP

May

Authorization & DSAWG Prep 1-3 weeks

Validity on security package (SSP/SAP/SAR/P OAM)

Review and Authorization

Authorization received, items / issues, vulnerability tables, & DSAWG brief developed

September

Mission Owners authorize use of a CSA utilizing the DoD Provisional Authorization MO guidance. After Authorization is issued, submit for connection

Final AO Review / PA Sign Off

Final AO Decision 1-2 weeks

Network Defense and Monitoring

Monitor & Manage

Authorizes use of CSA; Submit for Connection

DISA Review and Comments

Draft Authorization Recommendation / DSAWG Brief

DSAWG Review 1-2 weeks

DoD Review & Remediation

3PAO and CSP Document

3PAO conducts assessment

Validation begins (SSP/SAR/POA&M)

CSP/3PAO remediate issues, re-test, update documentation

Delivers revised package / Updates POA&M

Mission Owner

3PAO, remediation (if required)

JVT (Joint Validation Team) review of CSO package. Comments to CSP, 3PAO

Authorization & DSAWG brief developed

3PAO Assessment

DoD Review & Remediation

Estimated Review & Remediation duration is 11-17 weeks

3PAO Review and Proceed

Authorization & DSAWG Prep 1-3 weeks

3PAO and CSP Review and Approve SAP

SCA, JVT, and CSP Review and Approve SAP

Initial Contact Phase

DHRA Business Case Analysis

DLE Sponsor submits ICF to DISA

Onboarding Kickoff

DISA / DHRA holds process & requirements strategy meeting

April

DoD Review & Remediation 8-10 weeks

3PAO ASSESSMENT

SCA, JVT, and CSP review and approve SAP

May

Authorization & DSAWG Prep 1-3 weeks

Validity on security package (SSP/SAP/SAR/P OAM)

Review and Authorization

Authorization received, items / issues, vulnerability tables, & DSAWG brief developed

September

Mission Owners authorize use of a CSA utilizing the DoD Provisional Authorization MO guidance. After Authorization is issued, submit for connection

Final AO Review / PA Sign Off

Final AO Decision 1-2 weeks

Network Defense and Monitoring

Monitor & Manage

Authorizes use of CSA; Submit for Connection

DISA Review and Comments

Draft Authorization Recommendation / DSAWG Brief

DSAWG Review 1-2 weeks

DoD Review & Remediation

3PAO and CSP Document

3PAO conducts assessment

Validation begins (SSP/SAR/POA&M)

CSP/3PAO remediate issues, re-test, update documentation

Delivers revised package / Updates POA&M

Mission Owner

3PAO, remediation (if required)

JVT (Joint Validation Team) review of CSO package. Comments to CSP, 3PAO

Authorization & DSAWG brief developed

3PAO Review and Proceed

Authorization & DSAWG Prep 1-3 weeks

3PAO and CSP Review and Approve SAP

SCA, JVT, and CSP Review and Approve SAP

Initial Contact Phase

DHRA Business Case Analysis

DLE Sponsor submits ICF to DISA

Onboarding Kickoff

DISA / DHRA holds process & requirements strategy meeting

April

DoD Review & Remediation 8-10 weeks

3PAO ASSESSMENT

SCA, JVT, and CSP review and approve SAP

May

Authorization & DSAWG Prep 1-3 weeks

Validity on security package (SSP/SAP/SAR/P OAM)

Review and Authorization

Authorization received, items / issues, vulnerability tables, & DSAWG brief developed

September

Mission Owners authorize use of a CSA utilizing the DoD Provisional Authorization MO guidance. After Authorization is issued, submit for connection

Final AO Review / PA Sign Off

Final AO Decision 1-2 weeks

Network Defense and Monitoring

Monitor & Manage

Authorizes use of CSA; Submit for Connection

DISA Review and Comments

Draft Authorization Recommendation / DSAWG Brief

DSAWG Review 1-2 weeks

DoD Review & Remediation

3PAO and CSP Document

3PAO conducts assessment

Validation begins (SSP/SAR/POA&M)

CSP/3PAO remediate issues, re-test, update documentation

Delivers revised package / Updates POA&M

Mission Owner

3PAO, remediation (if required)

JVT (Joint Validation Team) review of CSO package. Comments to CSP, 3PAO

Authorization & DSAWG brief developed

3PAO Review and Proceed

Authorization & DSAWG Prep 1-3 weeks

3PAO and CSP Review and Approve SAP

SCA, JVT, and CSP Review and Approve SAP

Initial Contact Phase

DHRA Business Case Analysis

DLE Sponsor submits ICF to DISA

Onboarding Kickoff

DISA / DHRA holds process & requirements strategy meeting

April

DoD Review & Remediation 8-10 weeks

3PAO ASSESSMENT

SCA, JVT, and CSP review and approve SAP

May

Authorization & DSAWG Prep 1-3 weeks

Validity on security package (SSP/SAP/SAR/P OAM)

Review and Authorization

Authorization received, items / issues, vulnerability tables, & DSAWG brief developed

September

Mission Owners authorize use of a CSA utilizing the DoD Provisional Authorization MO guidance. After Authorization is issued, submit for connection

Final AO Review / PA Sign Off

Final AO Decision 1-2 weeks

Network Defense and Monitoring

Monitor & Manage

Authorizes use of CSA; Submit for Connection

DISA Review and Comments

Draft Authorization Recommendation / DSAWG Brief

DSAWG Review 1-2 weeks

DoD Review & Remediation

3PAO and CSP Document

3PAO conducts assessment

Validation begins (SSP/SAR/POA&M)

CSP/3PAO remediate issues, re-test, update documentation

Delivers revised package / Updates POA&M

Mission Owner

DoD Sponsor completes Initial Contact Forms. Meetings to review DLE requirements to determine best path to Provisional Authorization

Introduction, Team Briefs: Sponsor – Overview CSP – Architecture 3PAO – Assessment, Schedule & Plan SCCA – CAP NIC – IP & DNS DISA / DHRA priorities and notional schedule

Validation of CSO package. Comments to CSP, 3PAO, remediation (if required)
Support Reuse through the Learning Technology Warehouse

- Defense-wide Product Catalog of Authorized, Conformant, and Compliant systems for use in the DLR or by DoD stakeholders in their own environments
- Product Paged tie into DevSecOps pipeline and DLE operational dashboards to provide usage statistics to potential users.
- Automatically deploy demonstration capabilities / Rapidly deploy operational systems at time of need
- Scripts, widgets, and utilities to help migrate or interface with legacy systems
Learning Technology
Warehouse Demo
Questions and Discussion