16 June 2021

Implementing DevSecOps in MDA GMD

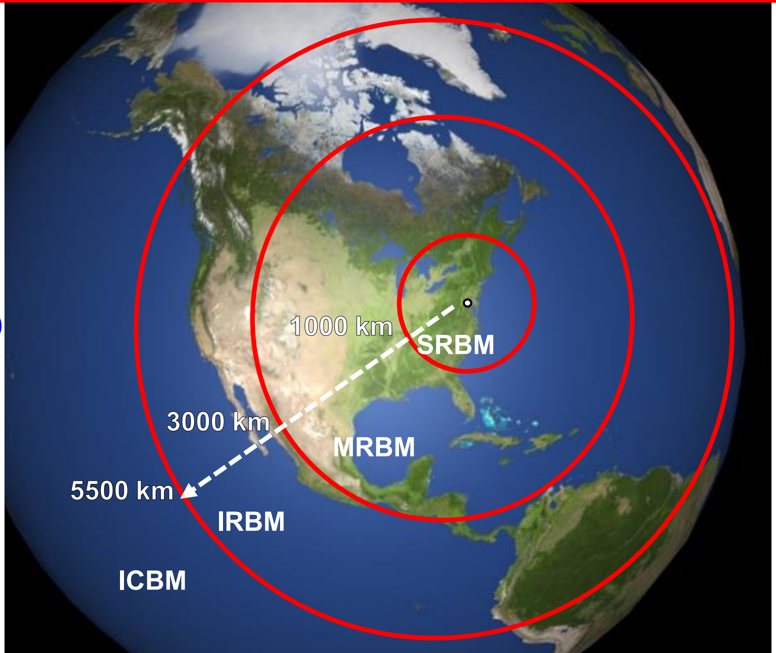
SEI DevSecOps Days

Ranjit S. Mann, PE
GMD DevSecOps Lead

Approved for Public Release
21-MDA-10845 (3 Jun 21)

Missile Defense
Evolving Threat Environment

Range



Note: Range rings from Pentagon to show scale

SRBM:	Short Range Ballistic Missile	(300-1000 km :: 621 mi)
MRBM:	Medium Range Ballistic Missile	(1000-3000 km :: 1864 mi)
IRBM:	Intermediate Range Ballistic Missile	(3000-5500 km :: 3418 mi)
ICBM:	Intercontinental Ballistic Missile	(5500+ km :: 3418+ mi)

Adversaries are fielding diverse and expansive ranges of modern offensive missile systems

- Developing new missiles & improving existing systems
  - Precision strike
  - Penetration aids (e.g. decoys, jamming devices)
- Capable of maneuvering in midcourse or terminal phase
  - Maneuvering Reentry Vehicle (MaRV)
  - Multiple Independent Reentry Vehicle (MIRV)
  - Hypersonic Glide Vehicle (HGV)
  - Long Range Cruise Missiles (Defense of Homeland)
- Integrating ballistic, cruise missiles and UAVs

Speed

Subsonic:	< Mach 1	(< 770 mph)
Supersonic:	Mach 1-5	(770-3,800 mph)
Hypersonic:	Mach 5-10	(3,800-7,700 mph)
High Hypersonic:	Mach 10-25	(7,700-19,200 mph)

North Korea
Hwasong-15 ICBM

Iran
Emad-1 MRBM with MaRV

China
DF-17 HGV

Russia
Kinzhal MRBM ALBM

Ref: 2019 Missile Defense Review

Approved for Public Release 21-MDA-10845 (3 Jun 21)

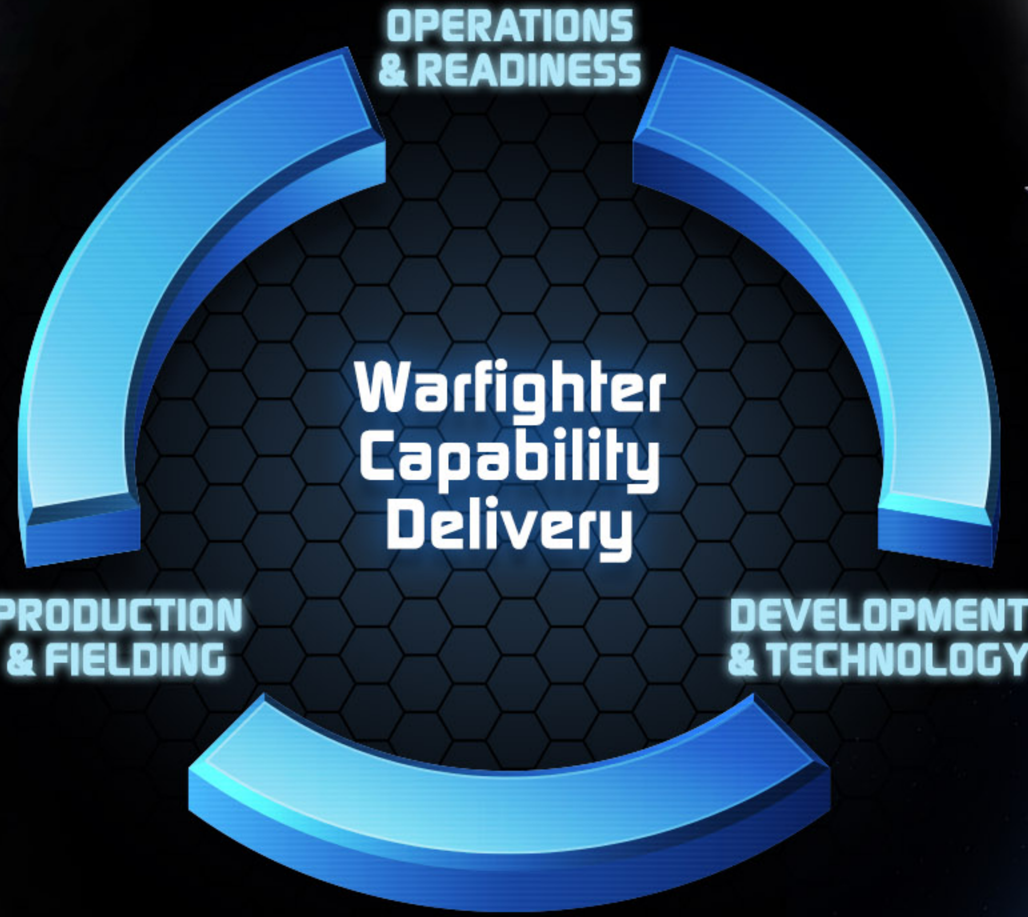
Missile Defense Agency Mission

To develop and deploy a layered Missile Defense System to defend the United States, its deployed forces, allies, and friends from missile attacks in all phases of flight

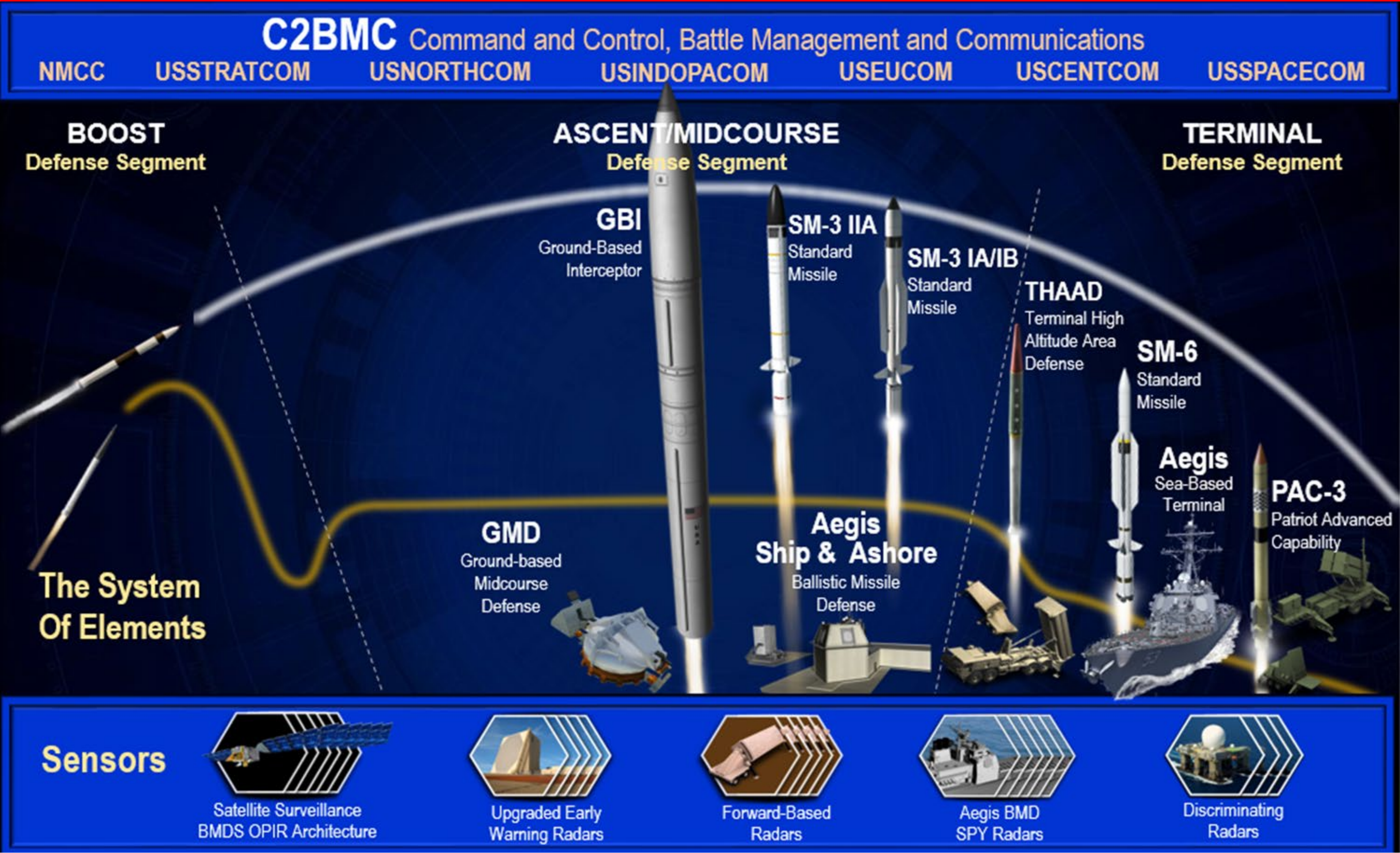
Missile Defense Capability Globally Deployed

Missile Defense Agency Foundations

In Support of Strategy to Defend the Nation



Today's Layered Active Missile Defense System



C2BMC Command and Control, Battle Management and Communications

NMCC USSTRATCOM USNORTHCOM USINDOPACOM USEUCOM USCENTCOM USSPACECOM

BOOST
Defense Segment

ASCENT/MIDCOURSE
Defense Segment

TERMINAL
Defense Segment

GBI
Ground-Based
Interceptor

SM-3 IIA
Standard
Missile

SM-3 IA/IB
Standard
Missile

THAAD
Terminal High
Altitude Area
Defense

SM-6
Standard
Missile

Aegis
Sea-Based
Terminal

PAC-3
Patriot Advanced
Capability

GMD
Ground-based
Midcourse
Defense

Aegis
Ship & Ashore
Ballistic Missile
Defense

The System
Of Elements

Sensors

Satellite Surveillance
BMDS OPIR Architecture

Upgraded Early
Warning Radars

Forward-Based
Radars

Aegis BMD
SPY Radars

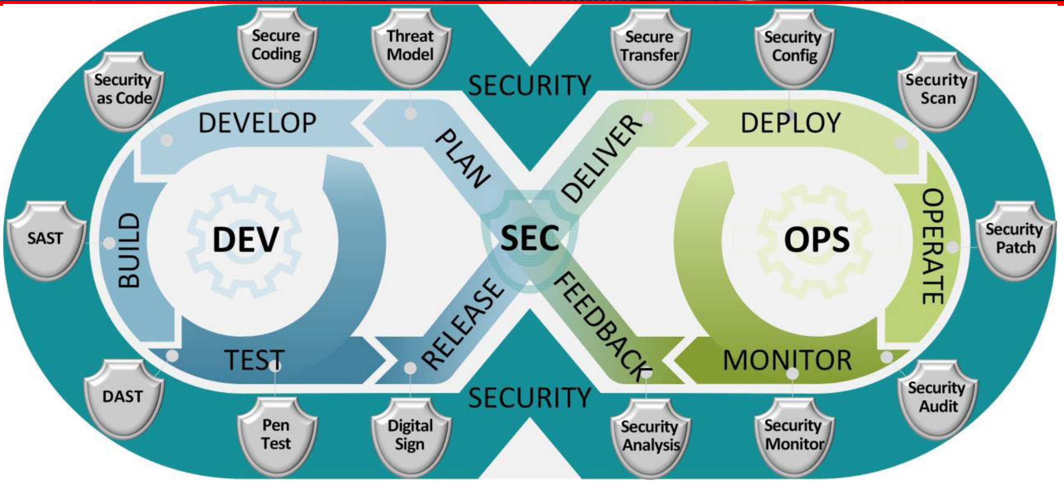
Discriminating
Radars

Approved for Public Release 21-MDA-10845 (3 Jun 21)

DoD Enterprise Development Security Operations (DevSecOps) Initiative

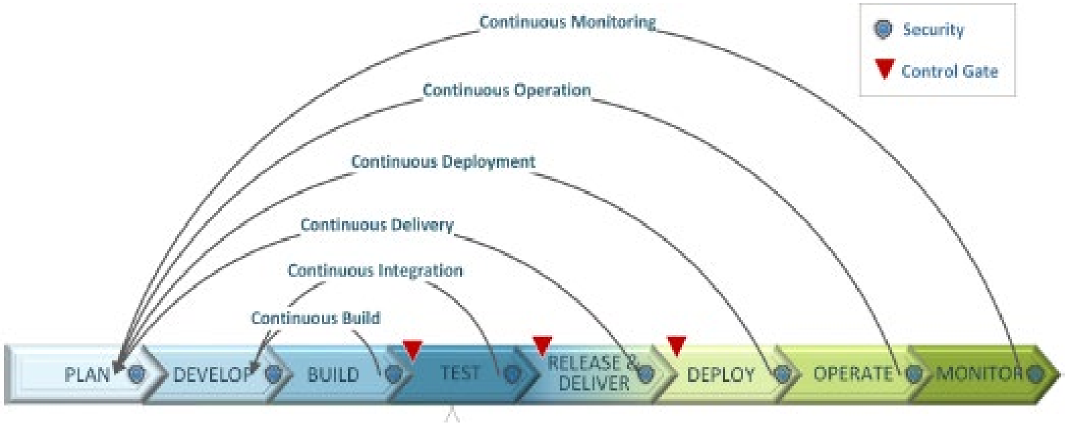
DevSecOps implementation value to MDA:

- ✓ Enhances Communication and Collaboration
- ✓ Continuous Integration / Continuous Delivery
- ✓ Rapid delivery of software capability to warfighter
  - Deploy software within days instead of months or years saving cost and schedule
- ✓ Implement cybersecurity earlier in software development life cycle (SDLC)
- ✓ Transparency into SDLC activities
- ✓ Reduces accreditation (Authority to Operate (ATO)) timeline from months to weeks or days by continuous ATO
- ✓ Increases software application portability
- ✓ Implements agile practices and principles in SDLC
- ✓ Hardware virtualization for early software and hardware integration (Find and Fix SW Bugs early)
- ✓ Enables automation to reduce the human error in SDLC



DevSecOps Software Lifecycle

Source: DoD Enterprise DevSecOps Reference Design (Sept 12, 2019)



Application DevSecOps Processes

Source: DoD Enterprise DevSecOps Reference Design (Sept 12, 2019)

Create, deploy, and operate software in a secure, flexible and interoperable manner via automated software tools, services and standards saving cost and schedule while achieving performance

Approved for Public Release 21-MDA-10845 (3 Jun 21)

DoD Leadership Thoughts On Software

"What keeps me up at night is not North Korea, but that the U.S. has lost it's ability to go fast."
- Gen Hyten as STRATCOM Commander at AFA in 2017

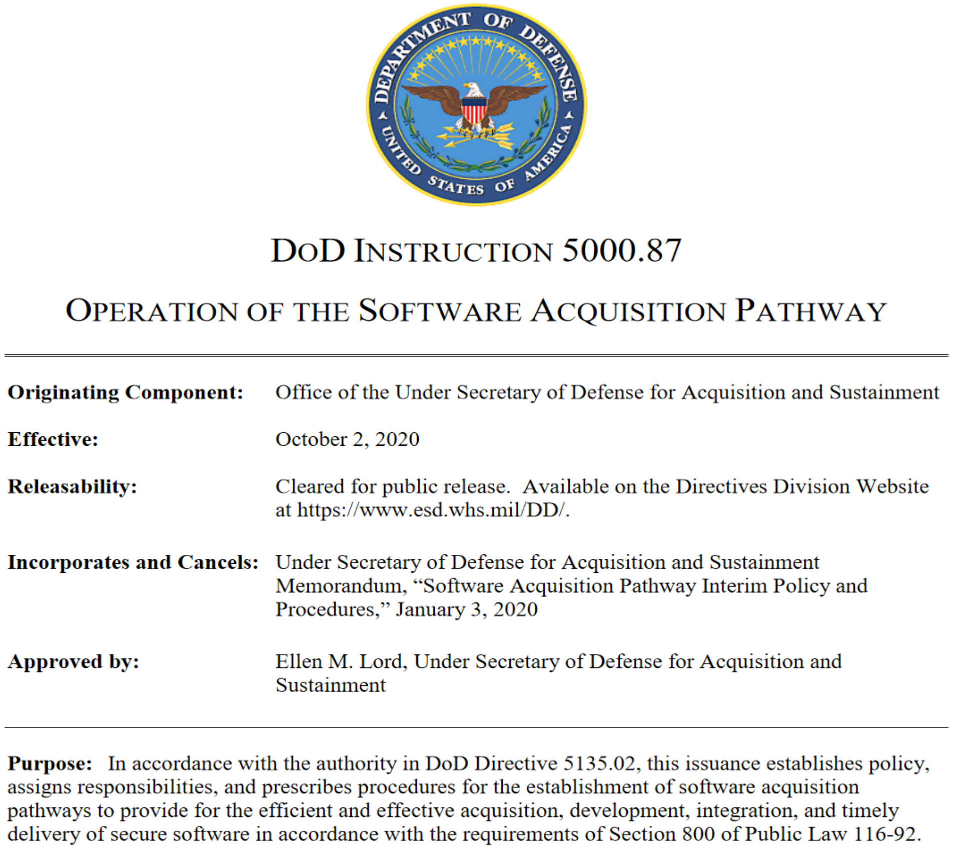
https://www.csis.org/events/conversation-general-john-hyten-vice-chairman-joint-chiefs-staff

"… the thread that runs through all of our programs and all that we do is software and I believe that we need to catch up with the private sector …" USD(A&S), HON Ellen Lord

Lets Talk Agile AAF Pathway with Sean Brady - Defense Acquisition University (dau.edu)

If confirmed to be the next USD(A&S), what is the first thing *you* would do to improve how DoD acquires software?

DoD DevSecOps Policy/Guidance



DoD Instruction 5000.87

Operation of the Software Acquisition Pathway

Originating Component: Office of the Under Secretary of Defense for Acquisition and Sustainment

Effective: October 2, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: Under Secretary of Defense for Acquisition and Sustainment Memorandum, "Software Acquisition Pathway Interim Policy and Procedures," January 3, 2020

Approved by: Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive 5135.02, this issuance establishes policy, assigns responsibilities, and prescribes procedures for the establishment of software acquisition pathways to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software in accordance with the requirements of Section 800 of Public Law 116-92.

1.2 Policy

Section (f) Programs will **require government and contractor software teams to use modern iterative software development methodologies (e.g., agile or lean), modern tools and techniques (e.g., development, security, and operations (DevSecOps))**, and human-centered design processes to iteratively deliver software to meet the users' priority needs.

Policy does not mandate DevSecOps but it is very difficult to meet policy without implementing DevSecOps

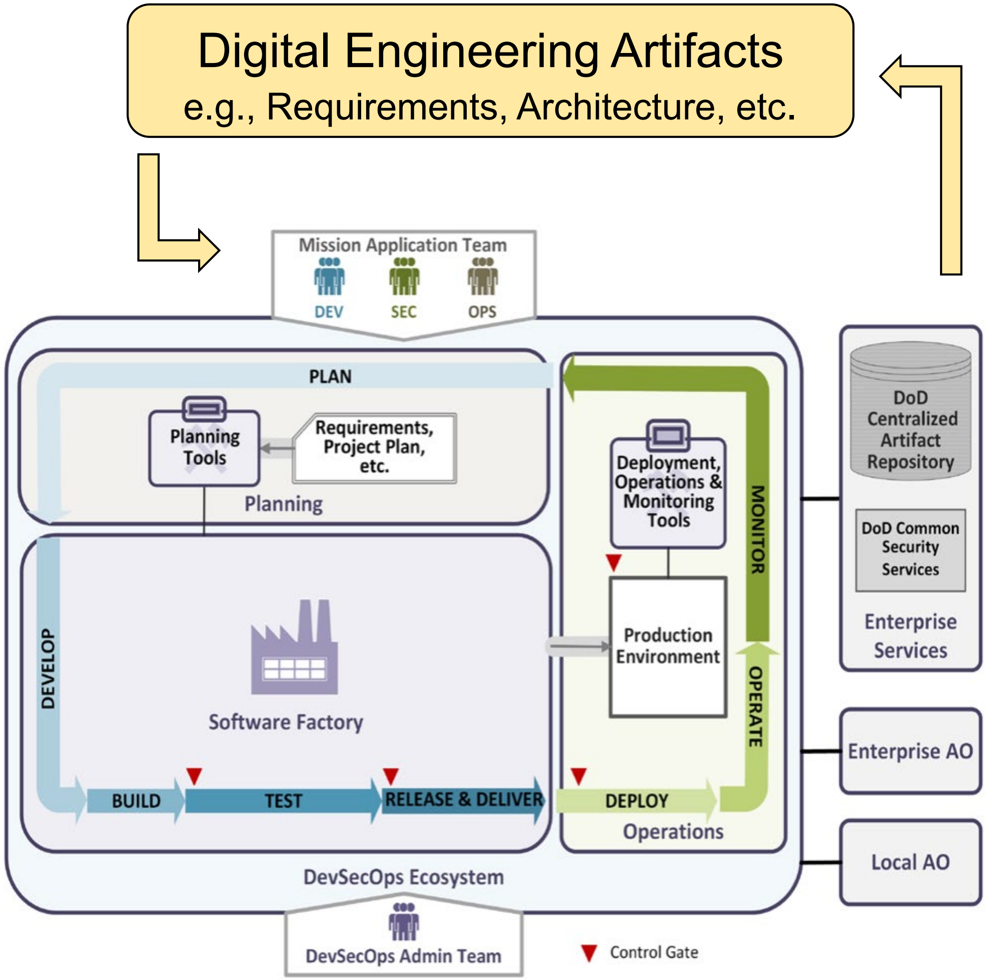
DevSecOps Overview

DevSecOps aims to ensure quick release cycles and promotes a collaborative, integrated communication platform … to include development, operational, compliance, tester, business analyst, project managers and end users who are sharing same business goals to maintain world class reliability, operation, and security.

Source: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=517144

DevSecOps

Digital Engineering



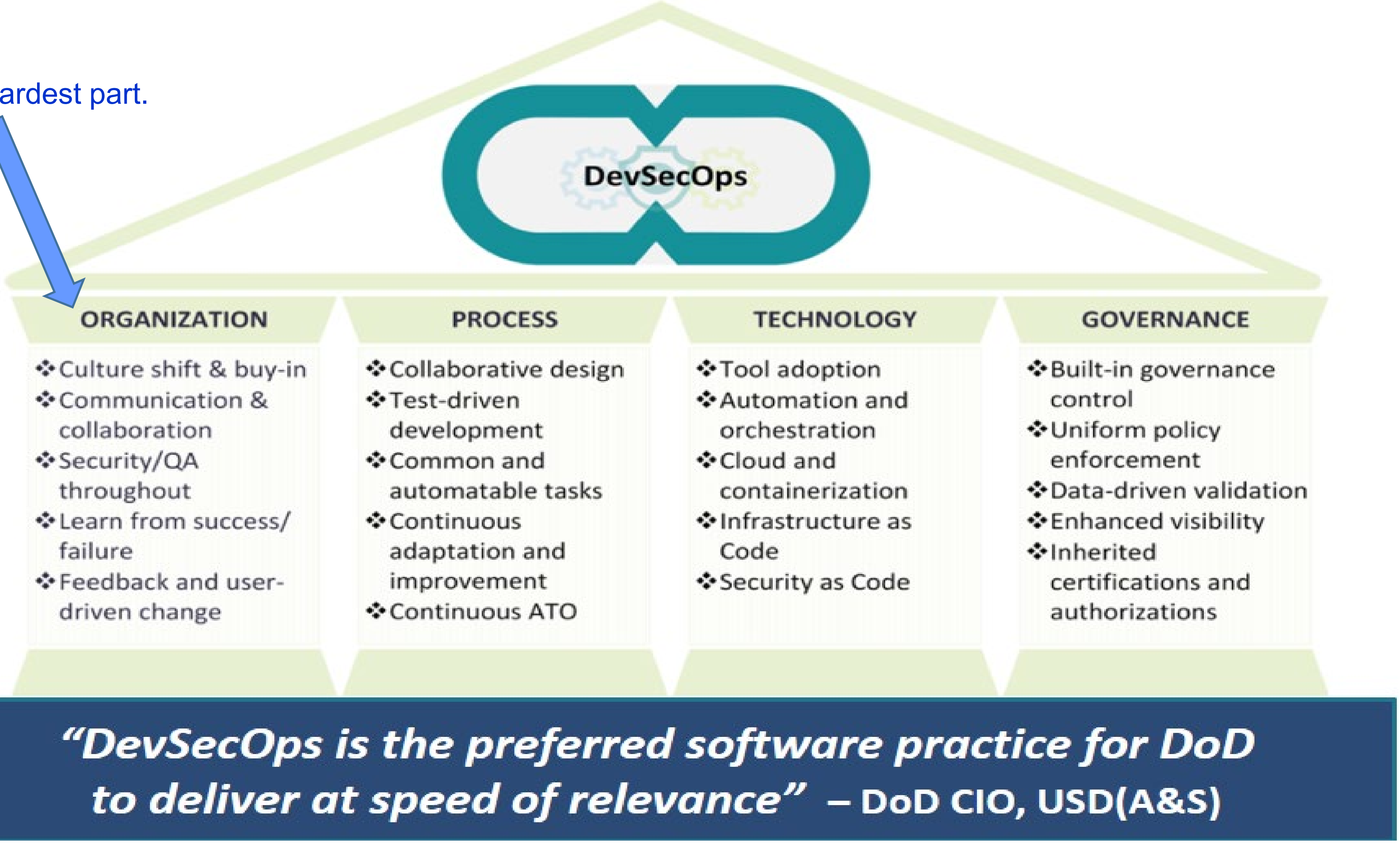
Digital Engineering Artifacts
e.g., Requirements, Architecture, etc.

Figure 8: DevSecOps Ecosystem

Source: DoD Enterprise DevSecOps Reference Design (Sept 12, 2019)

DevSecOps Reference Design Pillars

The hardest part.



ORGANIZATION

- Culture shift & buy-in
- Communication & collaboration
- Security/QA throughout
- Learn from success/ failure
- Feedback and user-driven change

PROCESS

- Collaborative design
- Test-driven development
- Common and automatable tasks
- Continuous adaptation and improvement
- Continuous ATO

TECHNOLOGY

- Tool adoption
- Automation and orchestration
- Cloud and containerization
- Infrastructure as Code
- Security as Code

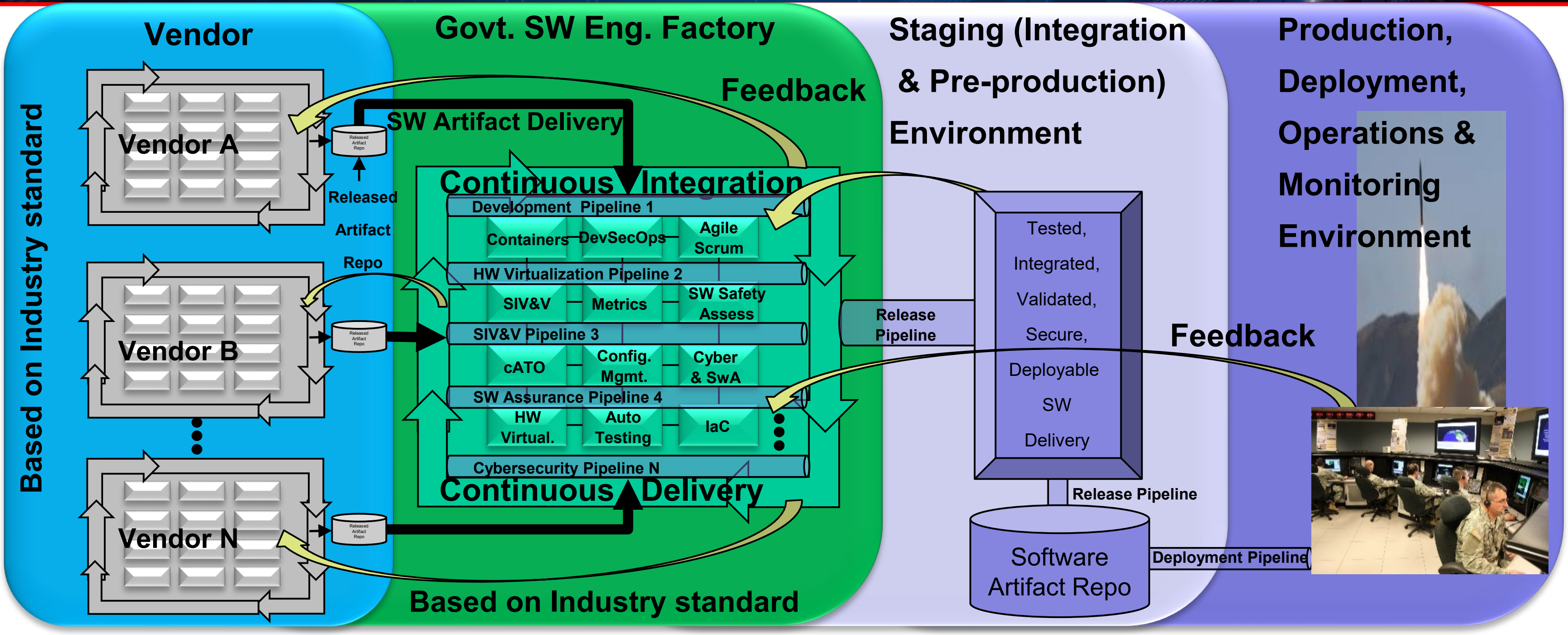
GOVERNANCE

- Built-in governance control
- Uniform policy enforcement
- Data-driven validation
- Enhanced visibility
- Inherited certifications and authorizations

> ***"DevSecOps is the preferred software practice for DoD to deliver at speed of relevance"*** **– DoD CIO, USD(A&S)**

DoD Enterprise DevSecOps Reference Design v1.0_Public Release.pdf (defense.gov)

SW DevSecOps Ecosystem Under Construction To Support GMD Programs - Vision



Vendor

Based on Industry standard

Vendor A

Vendor B

Vendor N

Released Artifact Repo

Govt. SW Eng. Factory

Feedback

SW Artifact Delivery

Continuous Integration

Development Pipeline 1

Containers

DevSecOps

Agile Scrum

HW Virtualization Pipeline 2

SIV&V

Metrics

SW Safety Assess

SIV&V Pipeline 3

cATO

Config. Mgmt.

Cyber & SwA

SW Assurance Pipeline 4

HW Virtual.

Auto Testing

IaC

Cybersecurity Pipeline N

Continuous Delivery

Based on Industry standard

Staging (Integration & Pre-production) Environment

Release Pipeline

Tested, Integrated, Validated, Secure, Deployable SW Delivery

Release Pipeline

Software Artifact Repo

Deployment Pipeline

Production, Deployment, Operations & Monitoring Environment

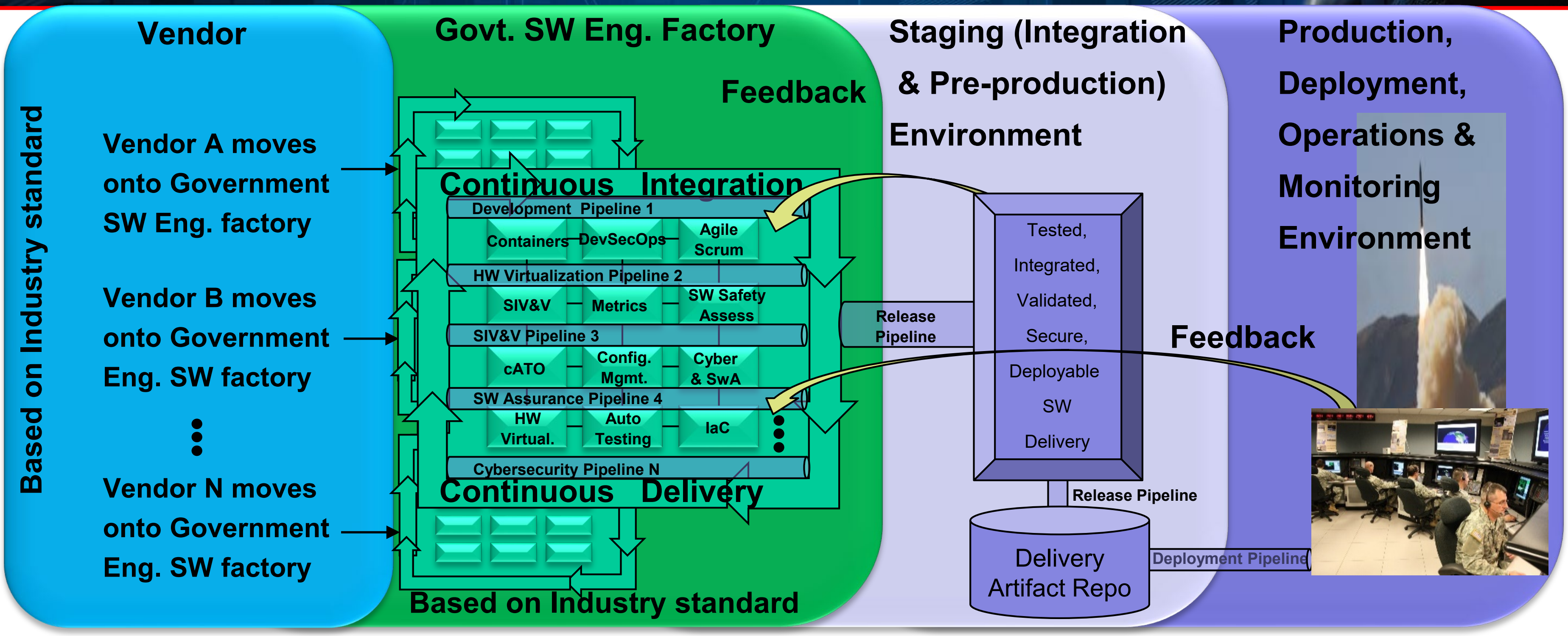
Feedback

DevSecOps Task	Vendor Env.	Gov. Env.	DevSecOps Task	Vendor Env.	Gov. Env.
Plan	✓	✓	Deliver	✓	✓
Develop	✓	Deferred	Deploy	NA	✓
Build	✓	✓	Operate	NA	✓
Test	✓	✓	Monitor	NA	✓
Release	✓	✓			

DevSecOps Software Functions Government & Industry Environment

Approved for Public Release 21-MDA-10845 (3 Jun 21)

SW DevSecOps Ecosystem Under Construction To Support GMD Programs - Vision



Vendor

Based on Industry standard

Vendor A moves onto Government SW Eng. factory

Vendor B moves onto Government Eng. SW factory

⋮

Vendor N moves onto Government Eng. SW factory

Govt. SW Eng. Factory

Feedback

Continuous Integration

Development Pipeline 1

Containers DevSecOps Agile Scrum

HW Virtualization Pipeline 2

SIV&V Metrics SW Safety Assess

SIV&V Pipeline 3

cATO Config. Mgmt. Cyber & SwA

SW Assurance Pipeline 4

HW Virtual. Auto Testing IaC

⋮

Cybersecurity Pipeline N

Continuous Delivery

Based on Industry standard

Staging (Integration & Pre-production) Environment

Release Pipeline

Tested, Integrated, Validated, Secure, Deployable SW Delivery

Release Pipeline

Delivery Artifact Repo

Deployment Pipeline

Feedback

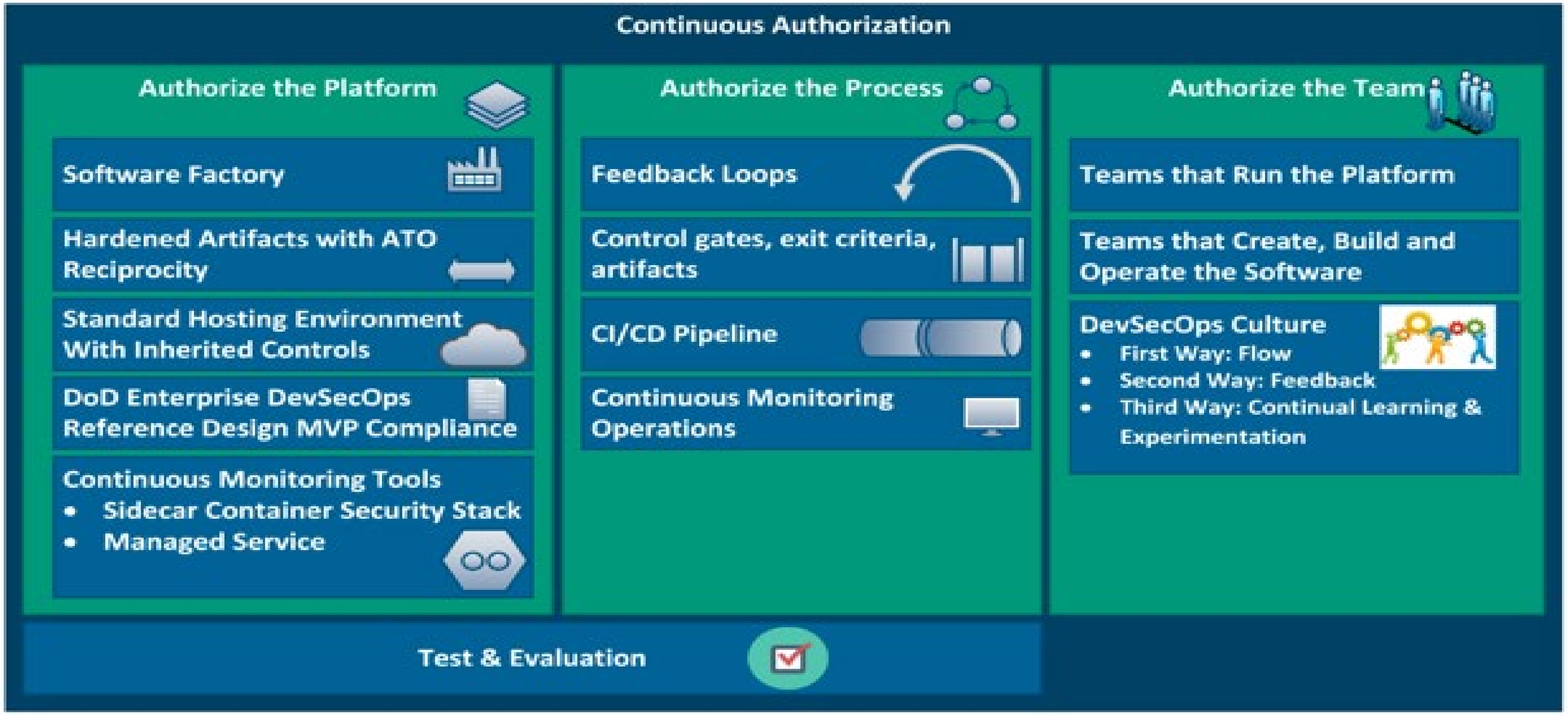
Production, Deployment, Operations & Monitoring Environment

DevSecOps Task	Vendor Env.	Gov. Env.	DevSecOps Task	Vendor Env.	Gov. Env.
Plan	Move to Gov. Env.	✓	Deliver	Move to Gov. Env.	✓
Develop	Move to Gov. Env.	✓	Deploy	NA	✓
Build	Move to Gov. Env.	✓	Operate	NA	✓
Test	Move to Gov. Env.	✓	Monitor	NA	✓
Release	Move to Gov. Env.	✓			

DevSecOps Software Functions in Government Environment

Approved for Public Release 21-MDA-10845 (3 Jun 21)

Continuous ATO (cATO)



Continuous Authorization

Authorize the Platform

- Software Factory
- Hardened Artifacts with ATO Reciprocity
- Standard Hosting Environment With Inherited Controls
- DoD Enterprise DevSecOps Reference Design MVP Compliance
- Continuous Monitoring Tools
  - Sidecar Container Security Stack
  - Managed Service

Authorize the Process

- Feedback Loops
- Control gates, exit criteria, artifacts
- CI/CD Pipeline
- Continuous Monitoring Operations

Authorize the Team

- Teams that Run the Platform
- Teams that Create, Build and Operate the Software
- DevSecOps Culture
  - First Way: Flow
  - Second Way: Feedback
  - Third Way: Continual Learning & Experimentation

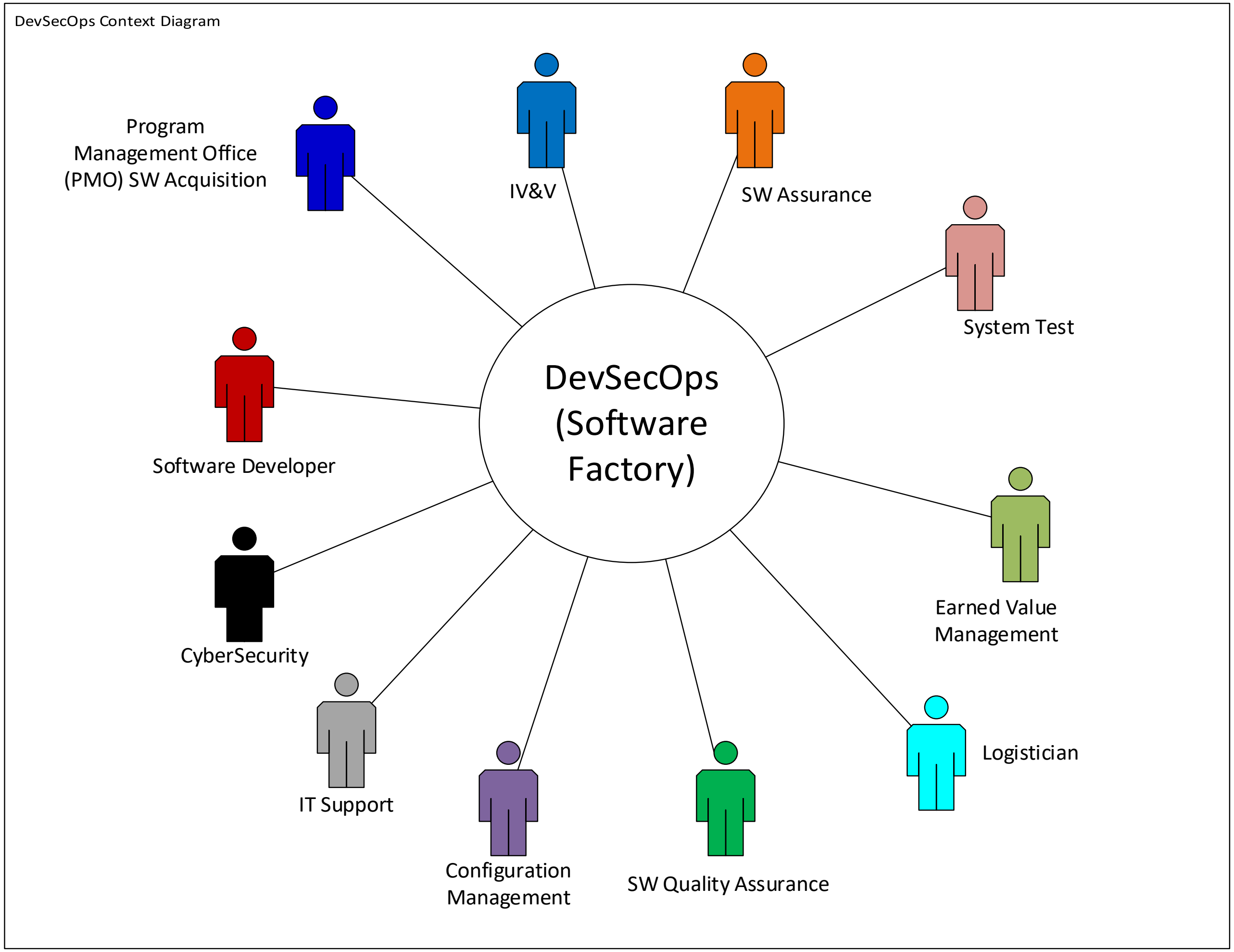
Test & Evaluation

https://repo1.dso.mil/dsawg-devsecops/continuous-ato-guidance/team6_documentation/-/tree/master/results/pdf <https://repo1.dso.mil/dsawg-devsecops/continuous-ato-guidance/team6_documentation/-/tree/master/results/pdf>

cATO authorizes the platform, process, and the team that produces the product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the Authorizing Official (AO)

Engagement with AO on regular basis is important

Defense Innovation Board (DIB) Study
Software is Never Done



DevSecOps Is a Multifunction Team Journey Not a Destination!

Approved for Public Release 21-MDA-10845 (3 Jun 21)

STELLAR TEAM / NOBLE MISSION

MISSILE DEFENSE AGENCY

DEPARTMENT OF DEFENSE