



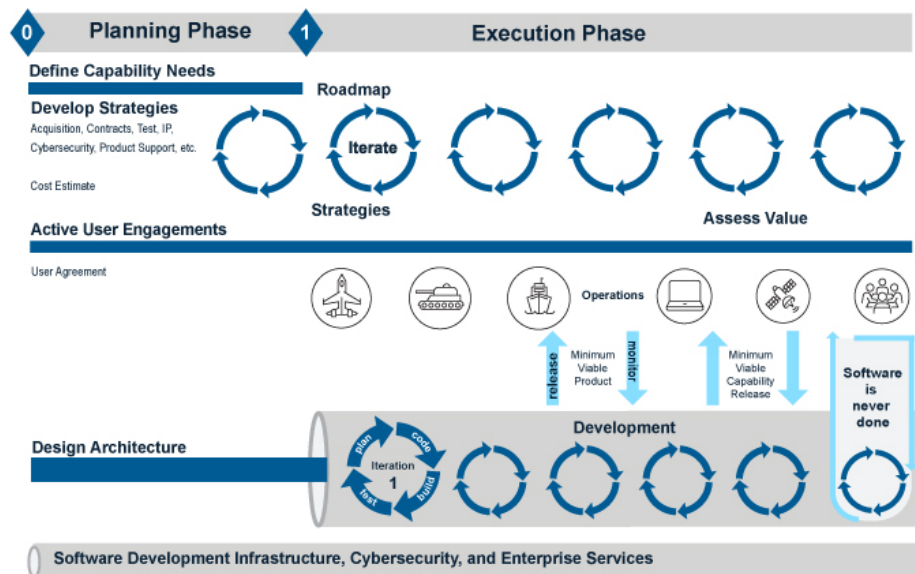
How Software Acquisition & DevSecOps Increase the Lethality of the DoD

neo@dod:~/\$ There is no spoon.

Sean Brady

DoD Senior Lead for SW Acq
USD(A&S)/Acq Enablers

1 Oct 2020

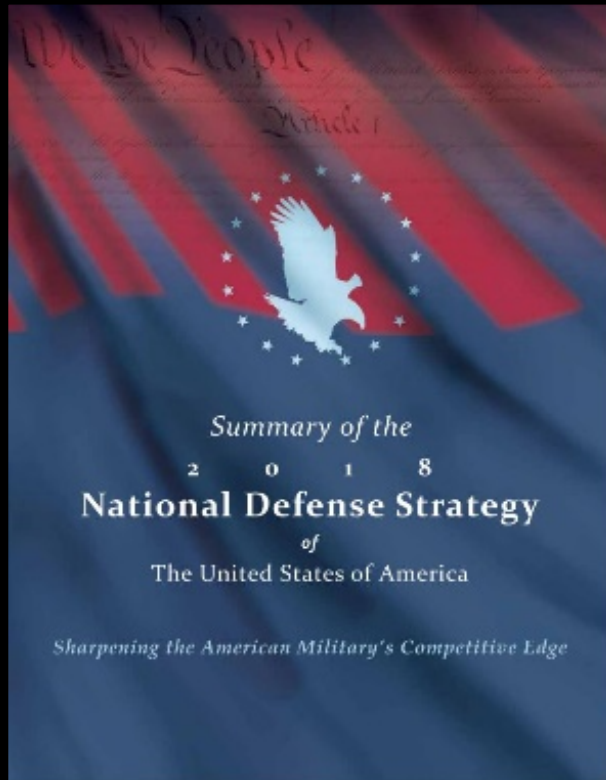


<https://aaf.dau.edu/aaf/software/>



There is no spoon in the SW ACQ pathway.

There is no spoon. There is no prioritization of regulatory bureaucracy and procedural bottlenecks either.

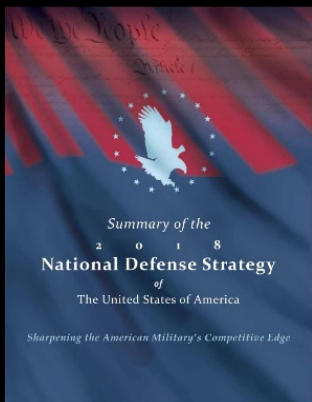


We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change. ■

National Defense Strategy



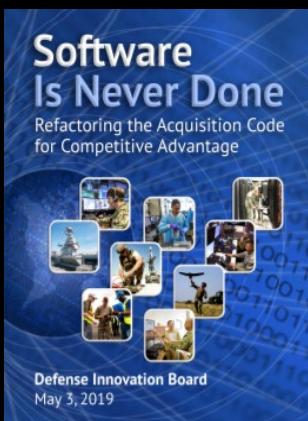
Urgency to Modernize. Faster is possible.



- ...prioritize speed of delivery, continuous adaptation, and frequent modular upgrades.



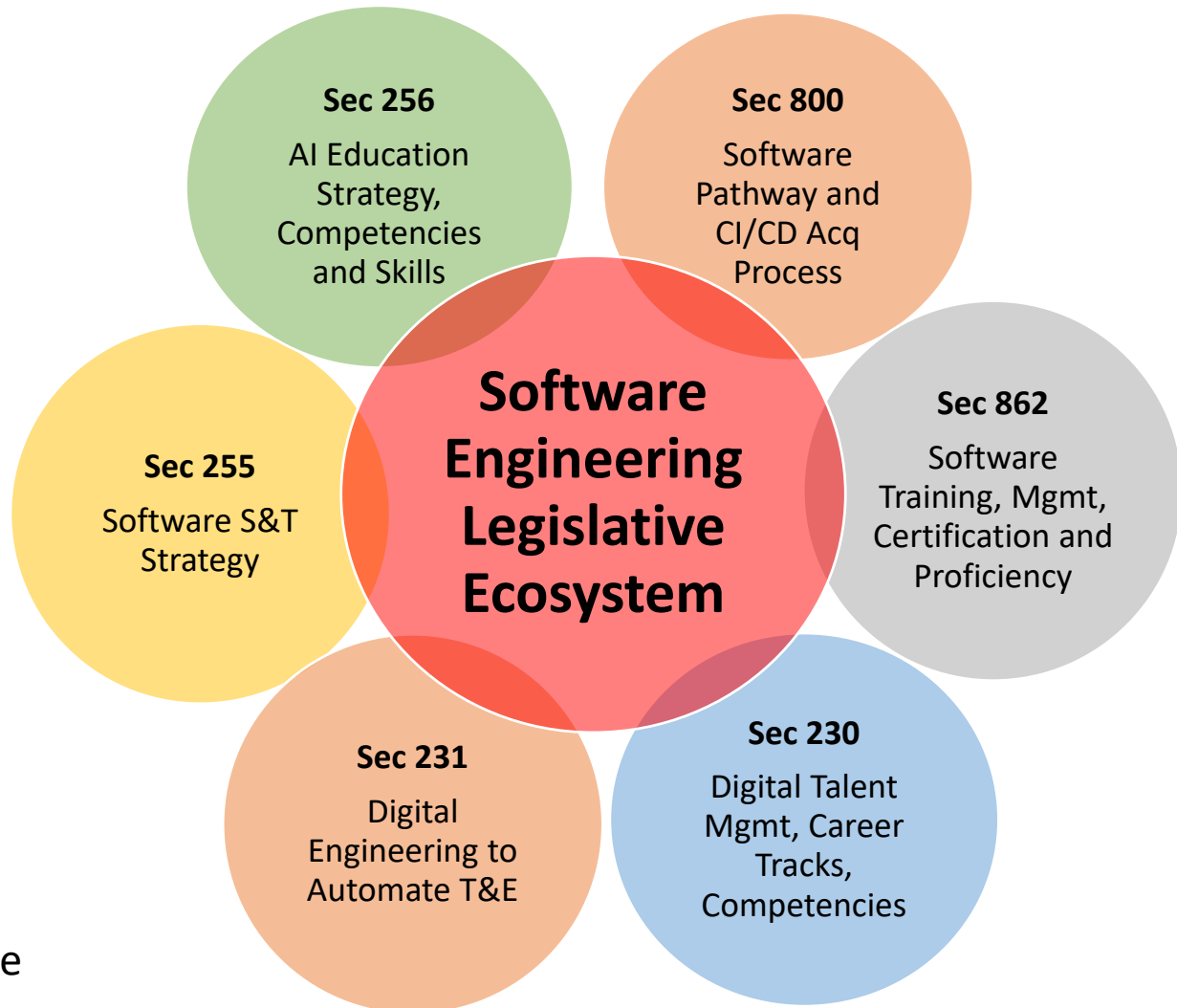
- **The Department must change.**
The United States must have the ability to update our systems rapidly.



- Speed & Cycle time matter.
Faster is more reliable. More Secure. Faster is possible.■



Congressional Direction to Modernize



Clear Signal:
Digitalization of the
DoD Workforce is a
National Security Issue



Approximating Commercial Industry

People

Process & Tech

Policy

**Software is eating
the world**

**Culture eats
strategy for
breakfast**

**Set the conditions
to unleash DSO**



“... 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



Gen Hyten - Vice Chairman of the Joint Chiefs of Staff

- 2nd priority: "do everything I can to **insert speed** into the processes inside the Pentagon."
- [our] processes are **not built for speed..they're built to remove risk.** ...a process designed to remove all risk, becomes **very structured, very bureaucratic.**
- The biggest thing we have to do in acquisition
 - **allow people to take risk** and **delegate the responsibilities** to people that are executing programs.
 - ...If you want to see a military person go fast, all you have to do is **give them the authority and responsibility**
- ...the **process that we have for building software is horrible.**



"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

Air Force's XQ-58A Valkyrie Attritable
Combat Drone



Army's Leader
Follower
Autonomous
Vehicle
Program

<https://www.autonews.com/shift/military-working-make-its-autonomous-technology-smarter>



Navy's Medium Displacement
Unmanned Surface Vehicle (MDUSV)



Navy's X-47B Unmanned
Combat Air System

<https://www.northropgrumman.com/what-we-do/air/x-47b-ucas/>



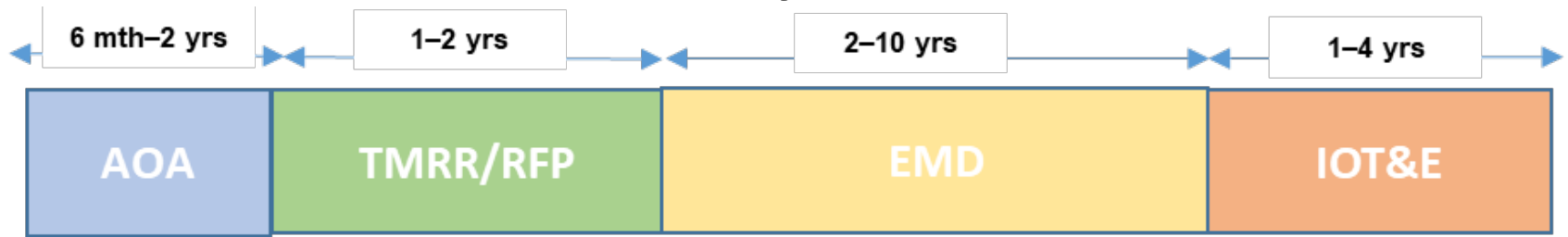
Army's Artificial
Intelligence for Maneuver
and Mobility, or AIMM

https://www.army.mil/article/236733/army_researchers_augment_combat_vehicles_with_ai



SW Delivery at the Speed of Relevance?


Old way?




DoD 5000.2



New Way?



The threat of the same-old, same-old pace is real. And the result is the U.S. is losing its technical edge to great-power competitors like China.



“We could be changing software every day as a necessary factor for winning.”



Software Acquisition Pathway

To facilitate rapid and iterative delivery of software capability to the user.

Source: DODI 5000.02 Section 4.2



<https://aaf.dau.edu/aaf/software/>



Key Elements of SW Acquisition Pathway

- Modern software development practices (Agile, DevSecOps, Lean)
- Capitalizing on active user engagement and enterprise services
- Software is rapidly and iteratively delivered to the operational environment to meet the highest priority user needs
- Tightly coupled mission-focused government-industry software teams
- Automated tools for development, integration, testing, certification



*Source: [DODI 5000.02](#)
[Section 4.2](#)*

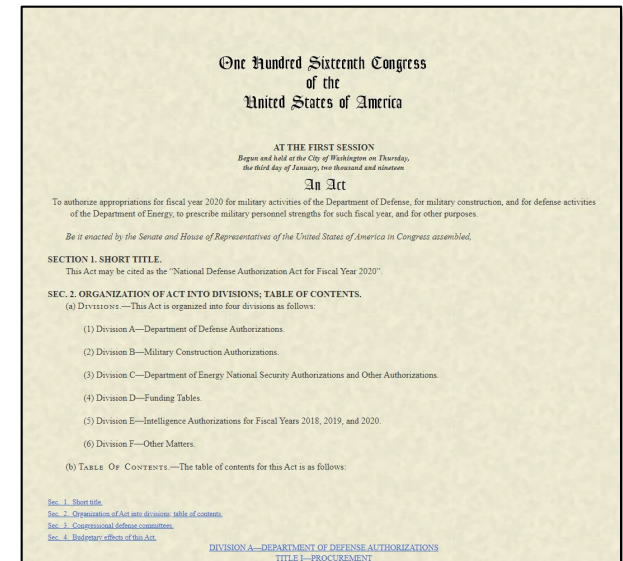


FY20 NDAA Section 800

Establish two pathways to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software

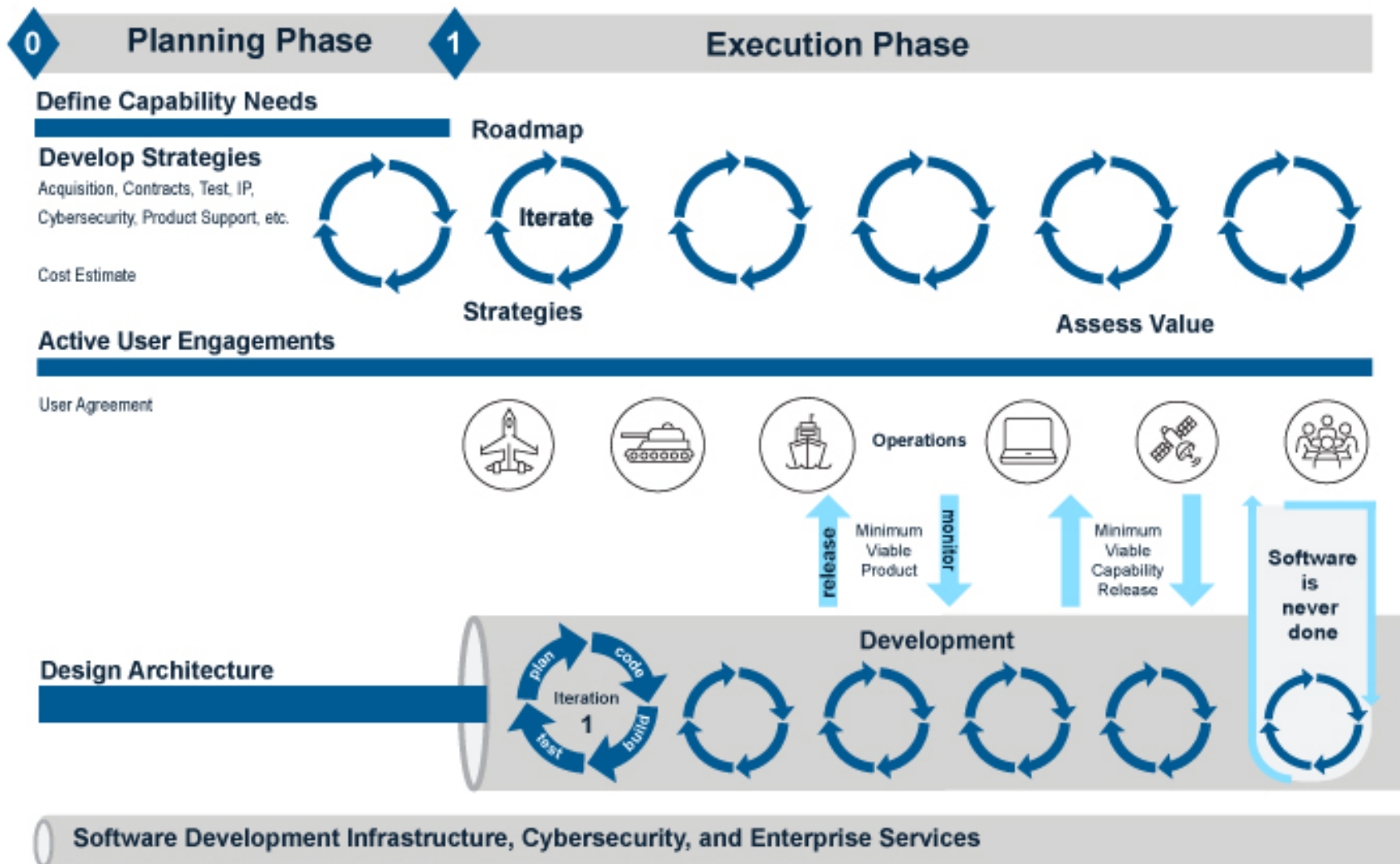
Applications and Embedded Systems

- Software programs shall not be treated as an MDAP
- Exempt from JCIDS (unless VCJCS, A&S, SAEs agree on new process)
- Streamline SW requirements, budget, acquisition processes
- Demonstrate viability and effectiveness of capabilities for operational use within one year after funds first obligated



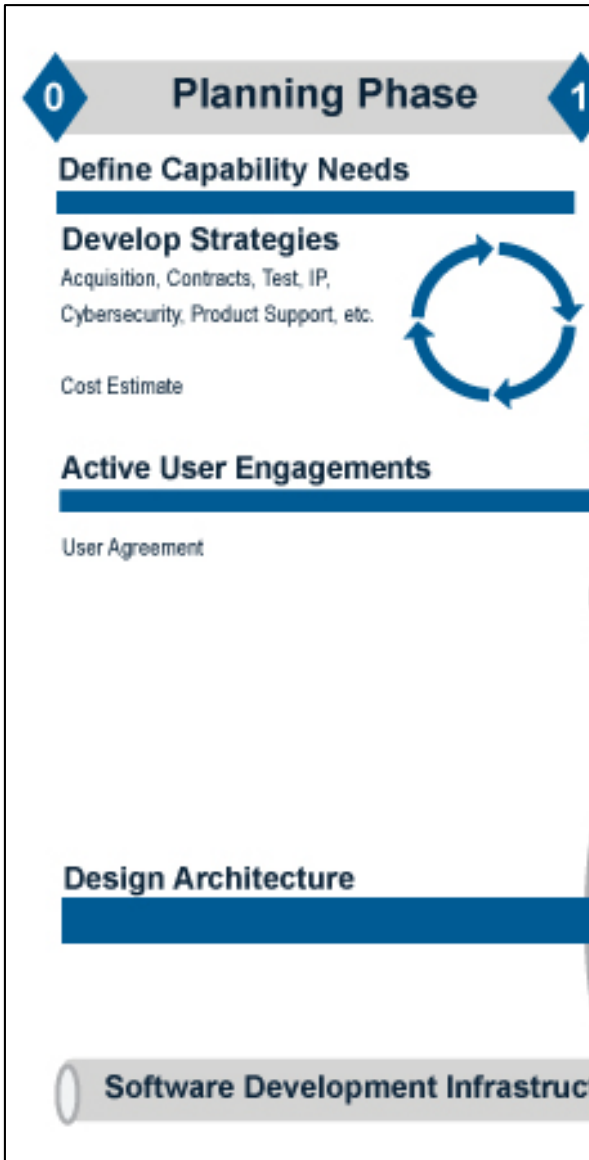


Software Acquisition Pathway





Planning Phase



Focuses on understanding the users' and systems' needs and planning the approach to deliver capabilities to meet those needs

Key Artifacts

- Capability Needs Statement
- User Agreement
- Program Strategies
- Cost Estimate



User Agreement

Agreement between the operational and acquisition communities to gain ensure active user involvement and decisions

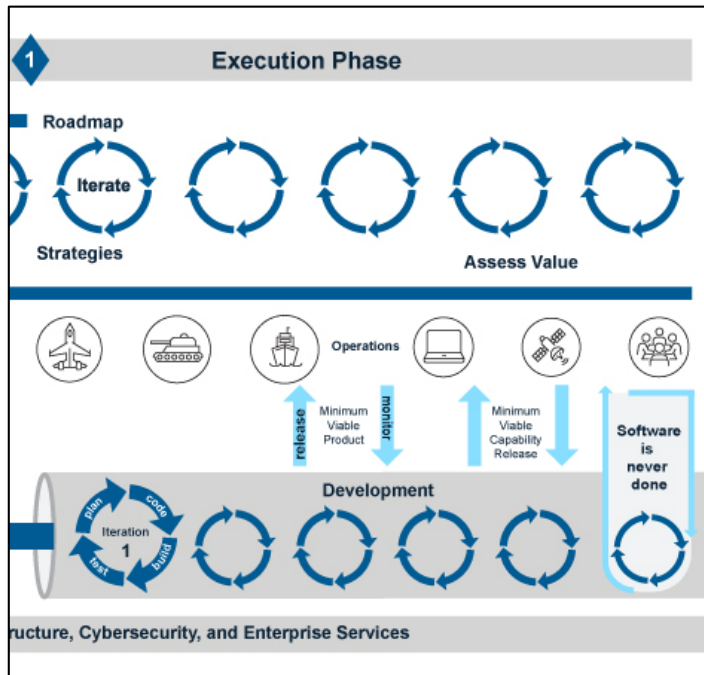


- Ensure proper resourcing of user involvement to support development
- Commit to active user involvement throughout design and development during planning phase
- Signed by sponsor, PMO prior to entry into Execution Phase

Establish Strong Ties to Users from Start



Execution Phase – Key Activities



Continuous improvement
of designs, services,
strategies, processes, and
capability deliveries to
maximize mission impact.

- **Product Roadmap**
 - Develop summary of planned releases over time
 - Create backlogs
- **Active User Engagements**
 - Understand ops environment, user feedback
- **Develop and Deliver Software**
 - Small, frequent releases to operations
 - Deliver MVP and MVCR within a year
 - Use Ent Services, DevSecOps pipeline
 - Engage T&E, Cyber, and Product Support
- **Track metrics; Assess value to users**



DSO Ref Design: Pillars

“preferred software practice for all DoD components to deliver at speed of relevance”
– DoD CIO, USD(A&S)

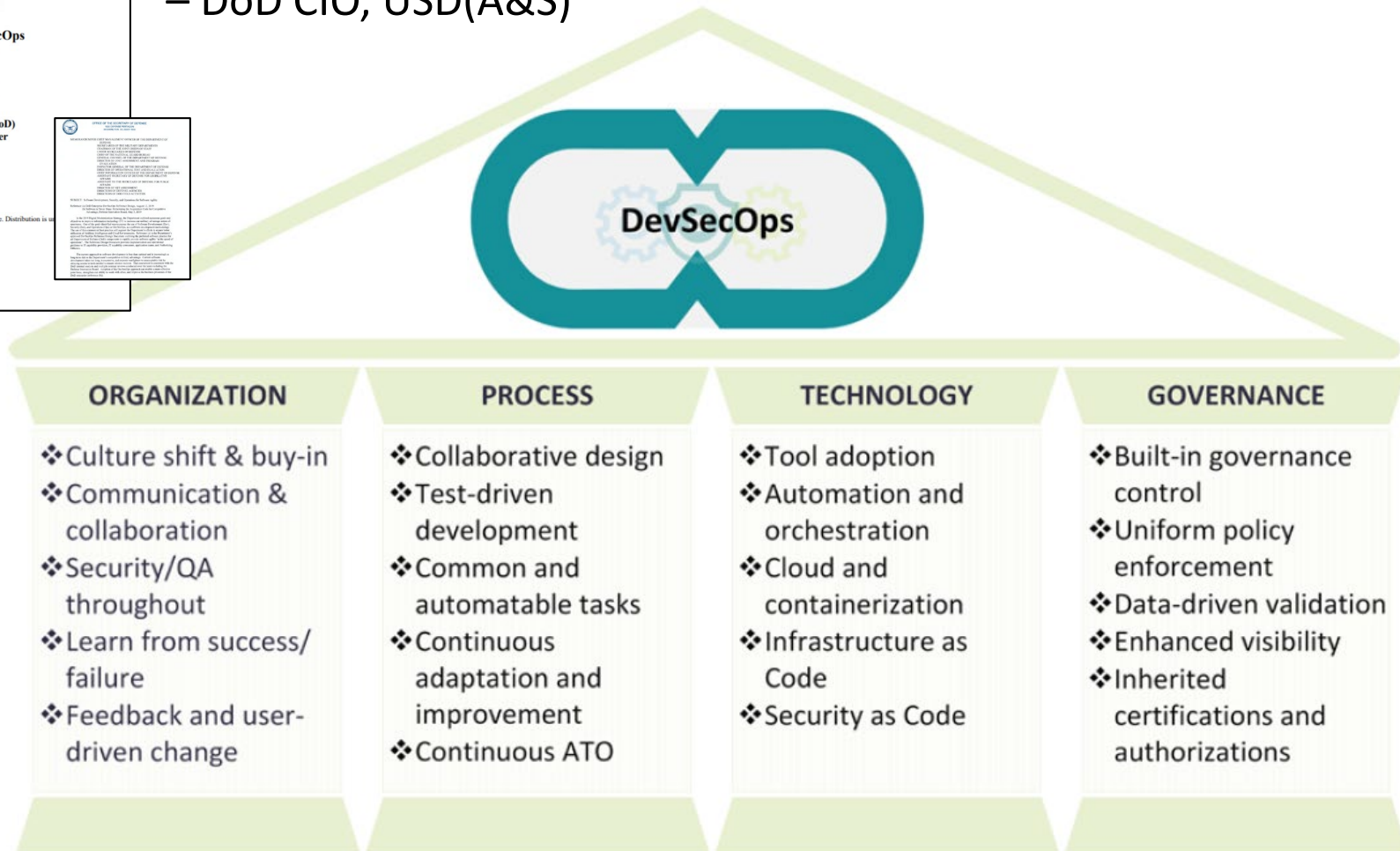
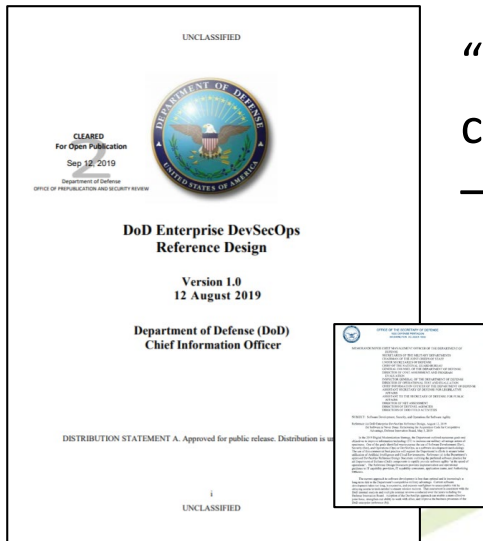


Figure 4: DevSecOps Pillars



JIDO – DevSecOps Enabling the Fight

Quantitative Impact:

Over a 6-month period, JIDO measured Key Performance Indicator (KPI) impact against pre- and post-DevSecOps enablement.

KPI	Definition	Legacy	DevSecOps Enabled	%/ \$ Impact
Availability Acceptable Quality Level (AQL)	Service Level Acceptable Quality Level (AQL) for Average Operational Availability of services	99.5%	99.9%	+3 HRS MONTHLY UPTIME
Continuous Authorization	Average time to complete code deployment after initial A&A	23 Days	6 Hours	92% FASTER
Deployment Frequency	The frequency new code reach customers	11	98 Releases	891% INCREASE
Initial System Authorization	Cybersecurity risk assessment threshold determination for pipeline including major system design and compliance with DoD Risk Management Framework	12 Months	3 Month	75% REDUCTION
Lead Time Reduction	The time from the start of a development cycle (the first new code) to deployment is the change lead time	169.83 Days	12 Days	93% REDUCTION
Mean Time to Provision	The average time that it takes to add additional services to an environment	6 Months	2 Hours	99.79% REDUCTION
Mean Time to Recovery	The average time from deployment failure to recovery	15.5 Minutes	4 Minutes	74% REDUCTION
Operating Cost	Change in operating costs based on leveraging open source tooling vs legacy COTs dependent architecture	\$1.8M	\$150K	91.66% REDUCTION

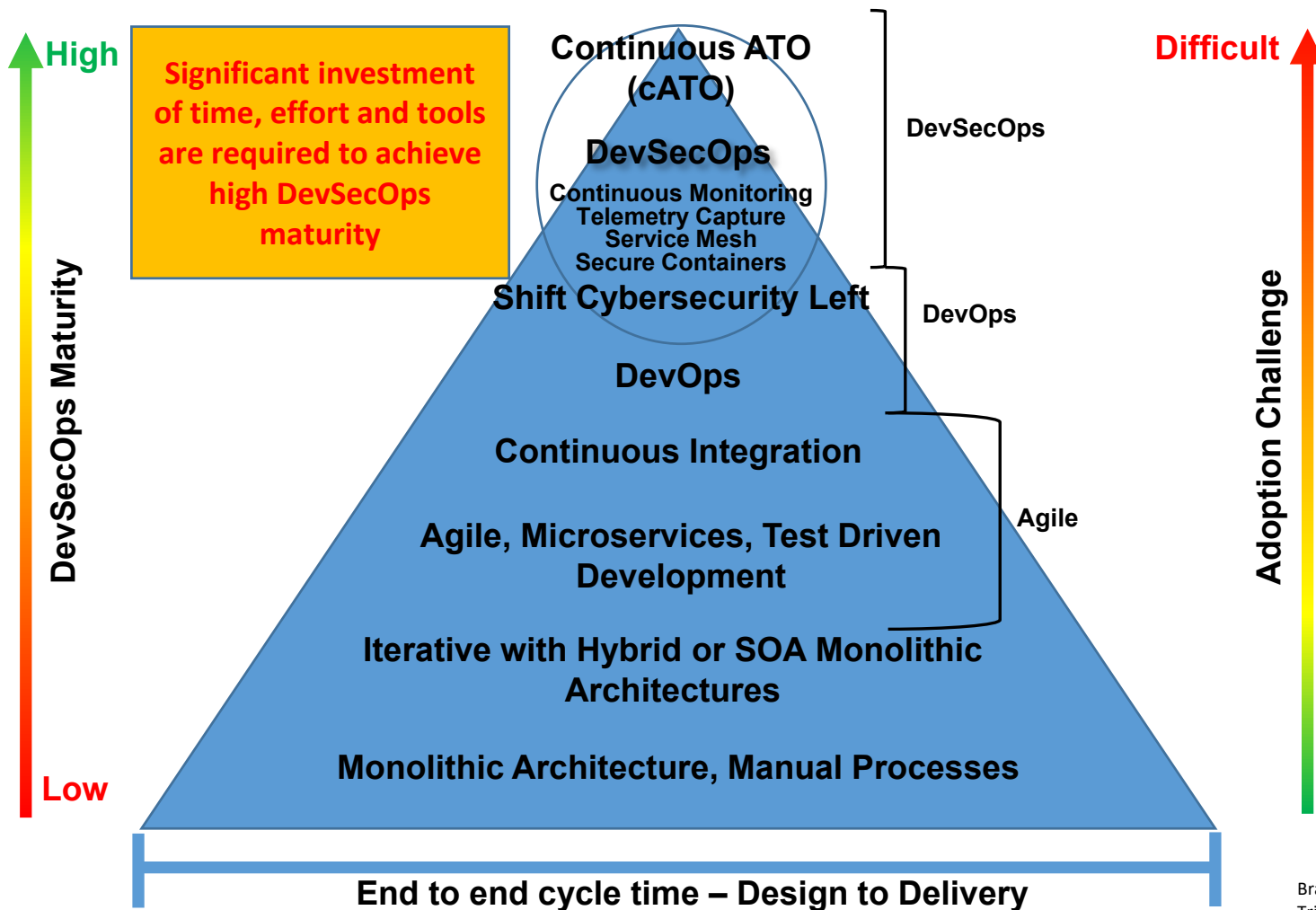




DevSecOps Maturity

Very Difficult to Adopt – Requires time - \$

Continuous ATO (cATO) enables bug and security fixes in minutes instead of months to years, and provides rapid deployment of critical capabilities to the war fighter at the speed of relevance.



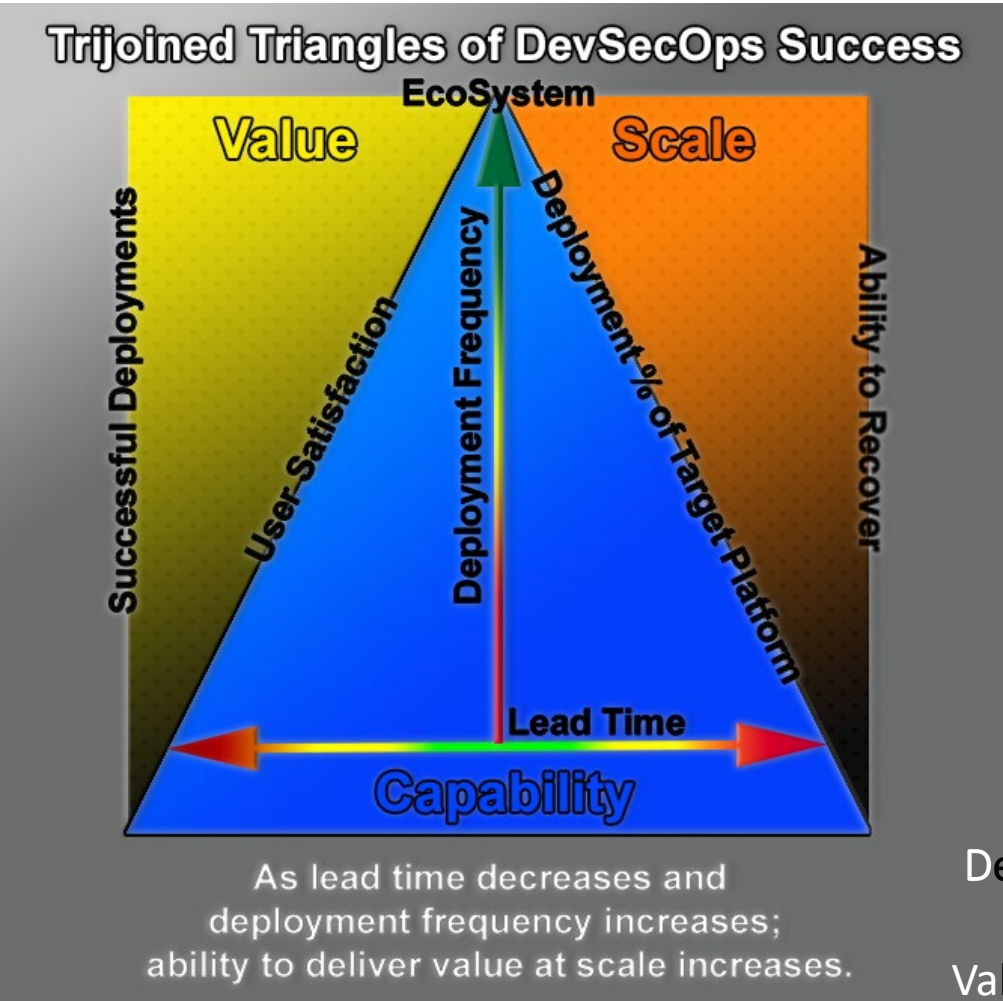


DevSecOps Success: Value@Scale

Delivery Throughput = [Lead Time] + [Deployment Frequency]

Value
[Failed Deployments] +
[Value to User]

Scale
[Mean Time To Recover] +
[% deployed to fleet]



“Enough prototyping already. How do we buy at scale?”
- GEN Hyten, VCJCS

DevSecOps BS DETECTOR:
Broken
Value/Availability/Delivery

Stark Brady Smith Trijoined Triangles of DSO Success



Benefits of Software Acquisition Pathway

- Tailored acquisition processes for software development
- No formal milestones – Delegated decision authorities
- Exempt from JCIDS (unless VCJCS, A&S, SAEs agree on new process)
 - Streamlined requirements process and iterative backlogs
 - Continue work with Joint Staff on a modified/expedited process
- Streamlined reviews & documentation requirements – No MDAPs
- Leverages enterprise services & not “rebuilding the factory” for every program
- Program tailoring and flexibility for Services/Agencies



Stay Engaged

Email: sean.p.brady.civ@mail.mil

AAF Website: <https://aaf.dau.edu/aaf/software/>

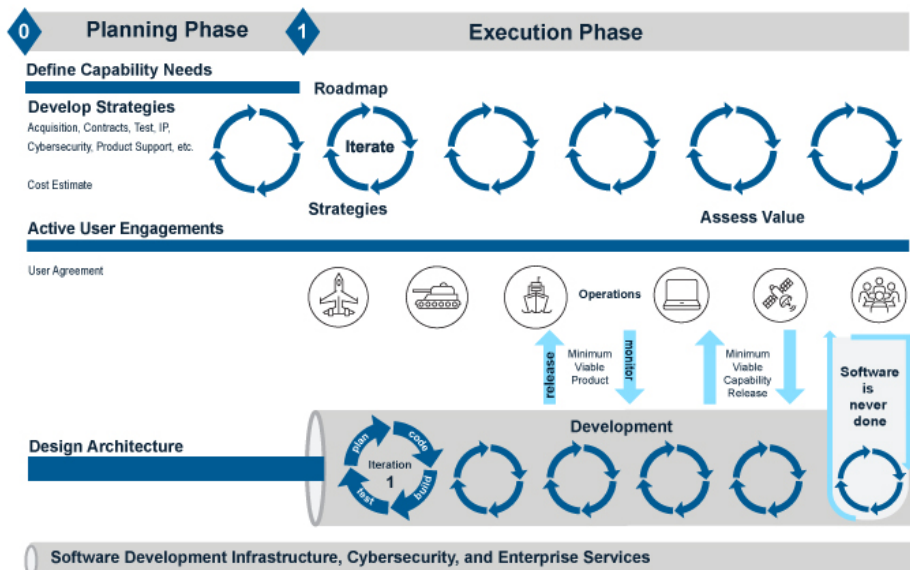
SW Pathway CoI: <https://www.milsuite.mil/book/groups/sw-pathway-community-of-interest>

Join our CoP Newsletter: <https://www.acq.osd.mil/ae/#/acquisition-approaches-management>

Sean Brady

**DoD Senior Lead for SW Acq
USD(A&S)/Acq Enablers**

Sep 2020

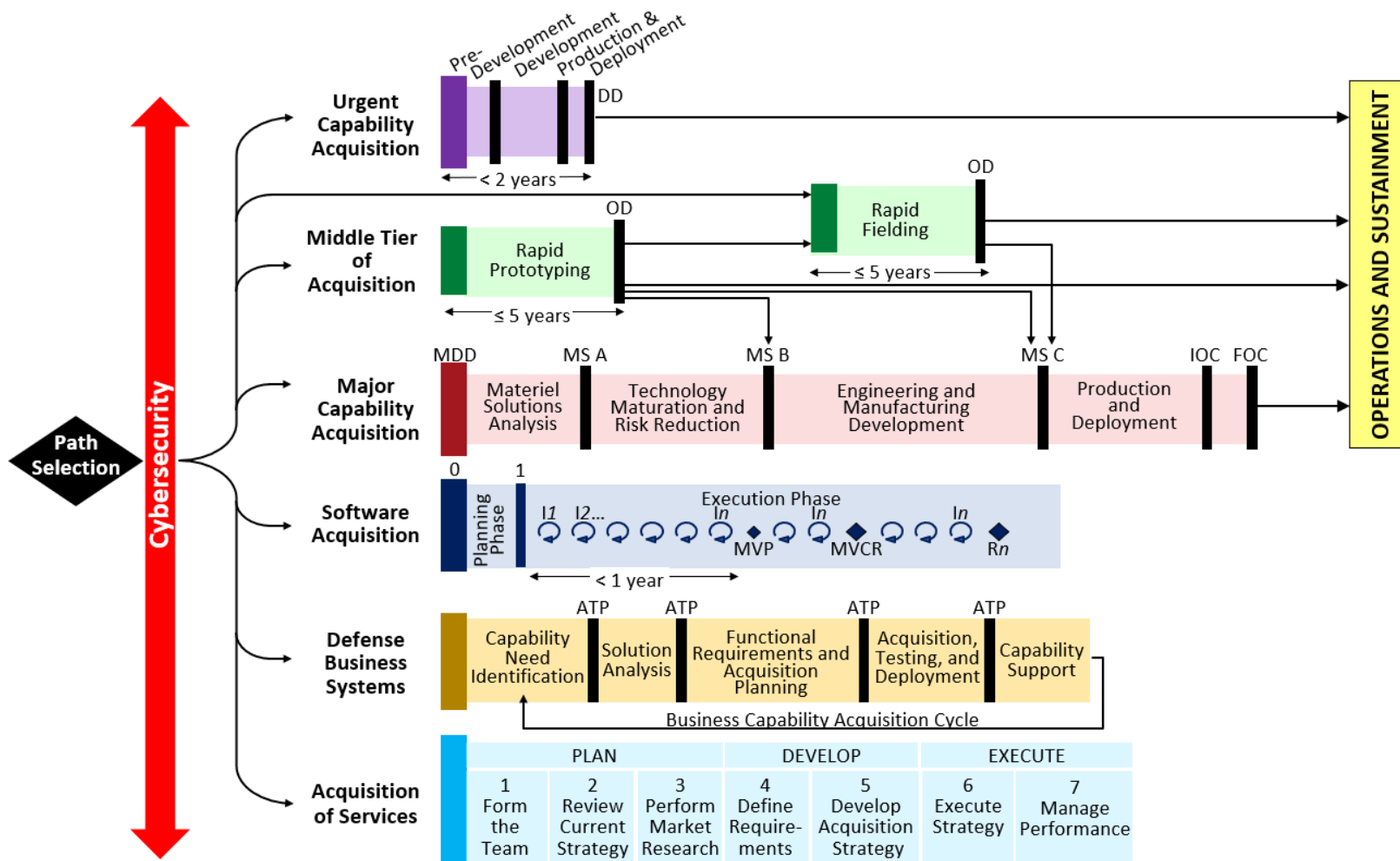




Backup Slides



Adaptive Acquisition Framework




A set of acquisition pathways to enable the workforce to tailor strategies to deliver better solutions faster.



Software Acquisition Pathway Policy

Interim Policy – 3 Jan 2020



THE UNDER SECRETARY OF DEFENSE
2010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

JAN 03 2020

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Software Acquisition Pathway Interim Policy and Procedures

Purpose. This interim policy establishes direction, responsibilities, and procedures for the management of the Software Acquisition Pathway pursuant to the authorities outlined in DoD Directive 5134.01, the July 13, 2018, Deputy Secretary of Defense Memorandum, and Section 800 of the National Defense Authorization Act for FY 2020. Further, this interim policy:

- Simplifies the acquisition model to enable continuous integration and delivery of software capability on timelines relevant to the Warfighter/end user.
- Establishes the Software Acquisition Pathway as the preferred path for acquisition and development of software-intensive systems.
- Establishes business decision artifacts to manage risk and enable successful software acquisition and development.

This interim policy will be replaced by issuance of a DoD Instruction within a year of signature of this memo.


Applicability. This interim policy applies to:

a) The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this interim policy as the "DoD Components").

b) Acquisition, development, operations, and sustainment of any DoD software-intensive system approved to use this pathway in order to demonstrate the viability and effectiveness of capabilities for operational use not later than one year after the date on which funds are first obligated to acquire or develop new software capability. Software-intensive systems include software-only systems, such as Command & Control (C2) software or applications; weapon system software, such as Intelligence, Surveillance, and Reconnaissance (ISR) software, embedded mission planning software or embedded Situational Awareness software; and any other custom-developed software running on commercial or modified commercial hardware. Software programs that meet the definition of a Defense Business System (DBS) and primarily acquire Commercial-Off-The-Shelf (COTS) components will follow DoDI 5000.75 procedures but may elect to use this pathway for custom developed software.



DODI 5000.UP – Fall 2020



DoD INSTRUCTION 5000.XX OPERATION OF THE
SOFTWARE ACQUISITION PATHWAY

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	Month Day, Year
Releasability:	Cleared for public release.
Approved by:	Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

In accordance with the authority in DoD Directive 5134.01 and the July 13, 2018 Deputy Secretary of Defense Memorandum, 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.

Provides initial structure and policies for software acquisition pathway. To be replaced by DODI in 1 year.

Interim Policy Memo

Final policy aligned with 5000 series, implements FY20 NDAA, insights from initial policy/pilots.

AAF Policies



Capabilities Needs Statement (CNS)

A high-level capture of need that provides enough information to define the software solution space, considering the threat environment.

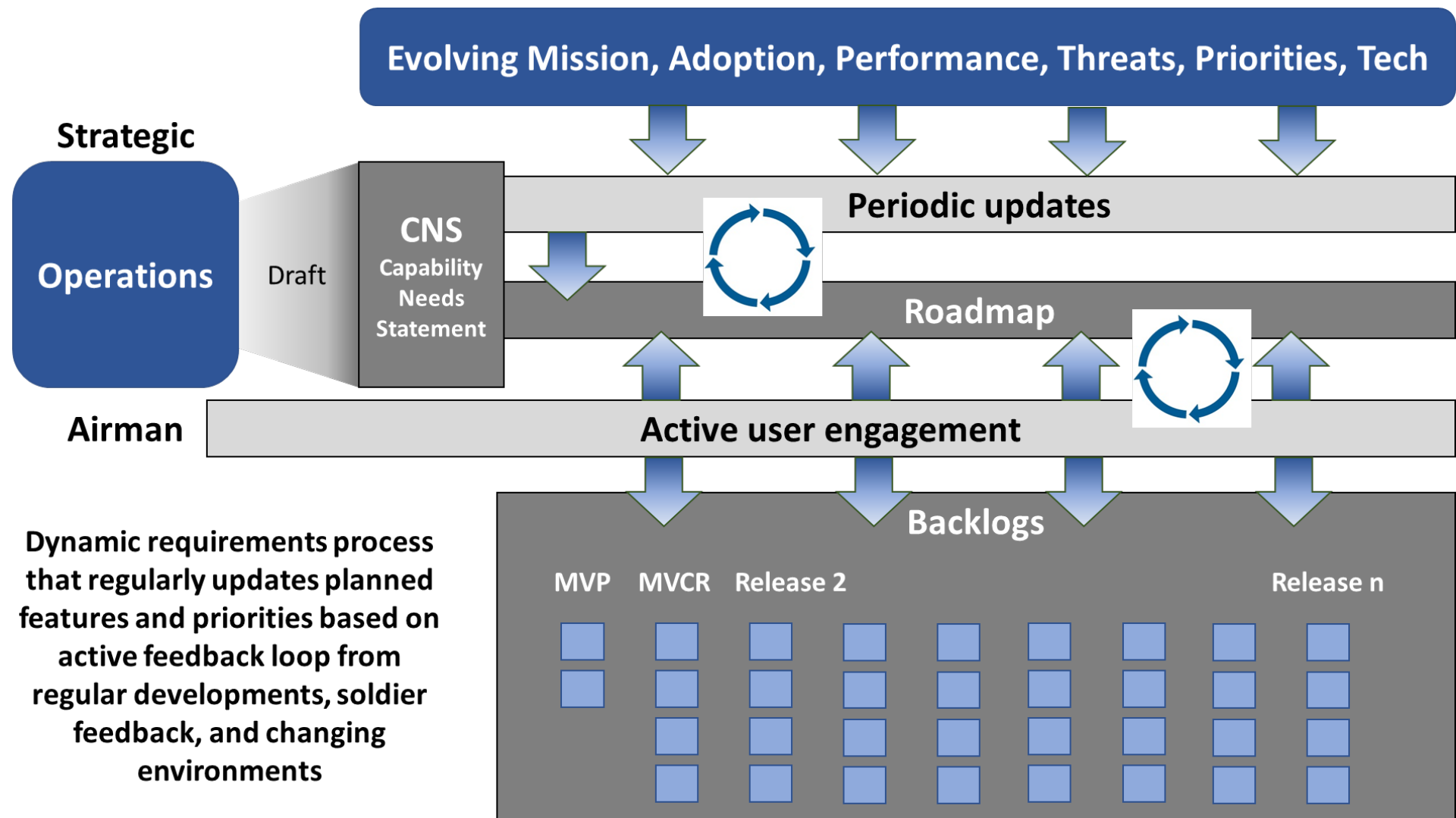
- Sponsor and Requirements Manager ID operational software capabilities needed
- Draft CNS to start the Software Pathway
- Refine during Planning Phase and approve prior to entry into Execution Phase



Clear Understanding of What is Needed



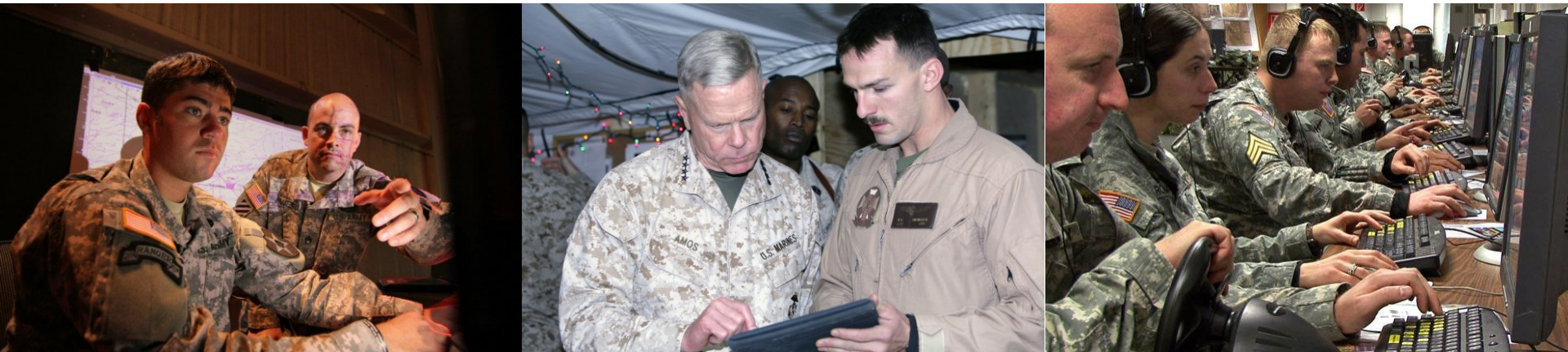
Evolving Software “Requirements”





Active User Engagements

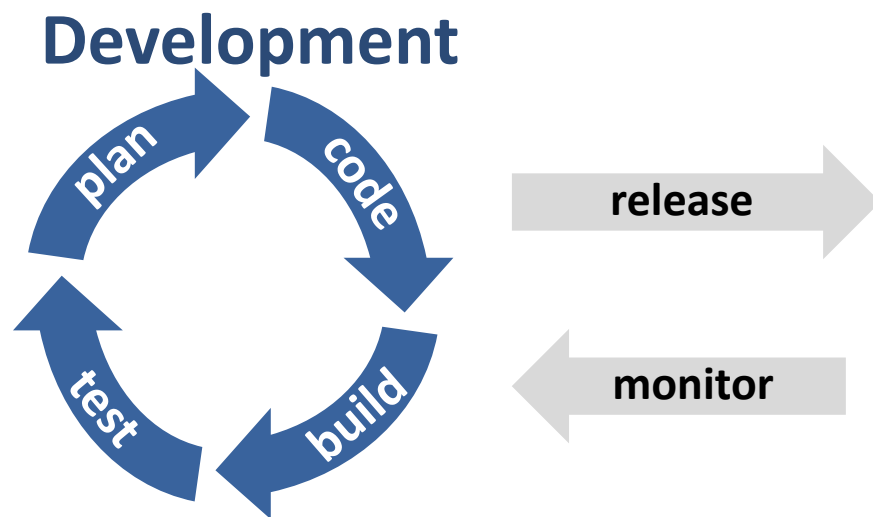
Critical to the success of software development to ensure delivered software address their priority needs



- Understand their needs and operational environment
- Solicit their feedback on MVPs, designs, developments



Develop and Deliver Software



Operations

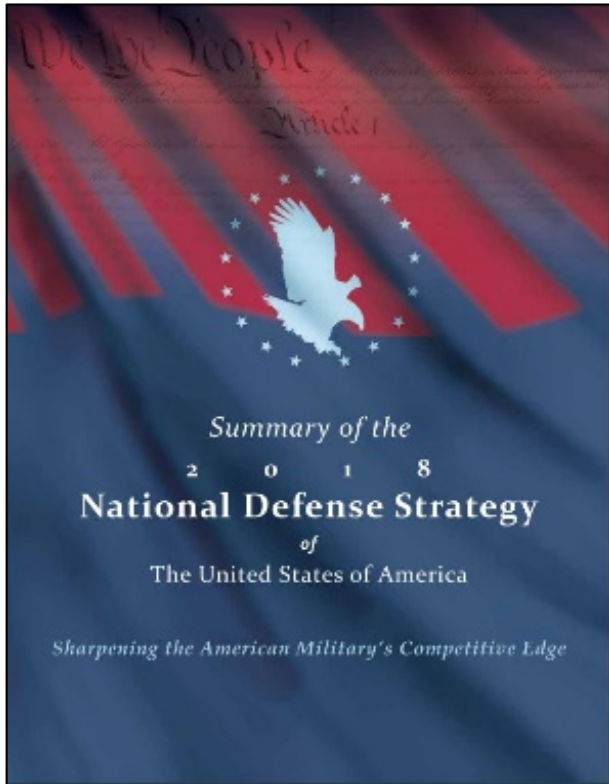


Software Development Infrastructure, Cybersecurity, and Enterprise Services

- Small, frequent releases
- Tailored software team's practices (Agile, DevSecOps)
- Heavily integrated, automated testing, cybersecurity
- Leverage enterprise services, DevSecOps pipelines



National Defense Strategy



National Defense Strategy

“Deliver performance at the speed of relevance.”

“Prioritize speed of delivery, continuous adaptation, and frequent modular upgrades.”

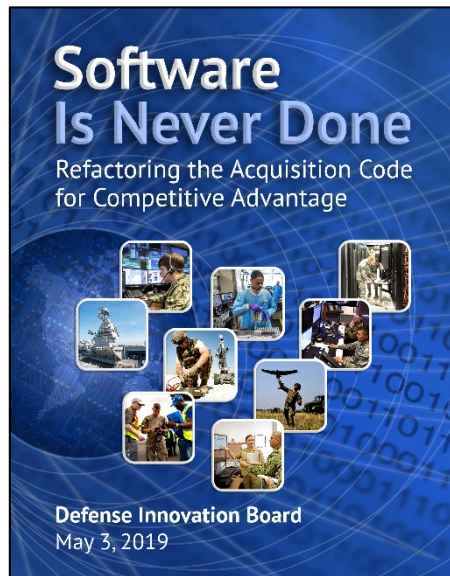
“Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting.”

“What keeps me up at night is ... that the U.S. has lost it’s ability to go fast.”
Software Acquisition Pathway and DevSecOps provides the framework (people, process, tools, and policy) that prioritizes speed and adaptability to win a future fight



Strategic Shaping of SW Acq Pathway

Defense Innovation Board (DIB) SWaP Study



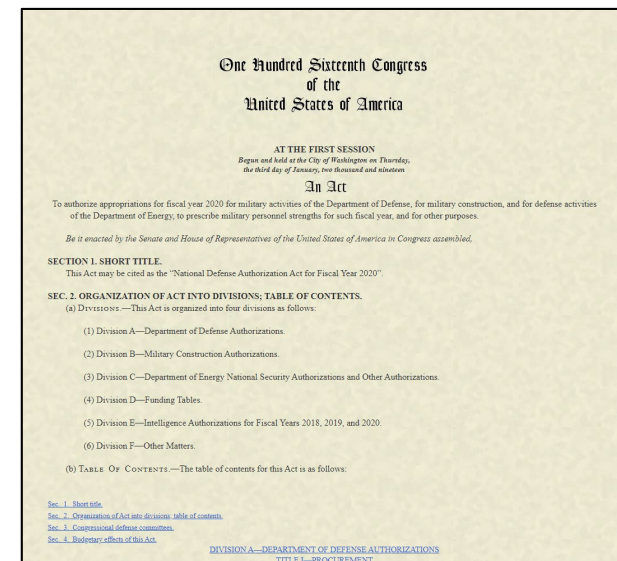
Speed and cycle times are top metrics

Congressionally driven Agile Pilots



Pilot Agile with flexibility on new, struggling programs

FY20 NDAA Section 800



Exempt from JCIDS*, MDAP, streamline processes, deliver within 1 year

*Unless new process developed



Two Paths within Software Acq Pathway

Application Path

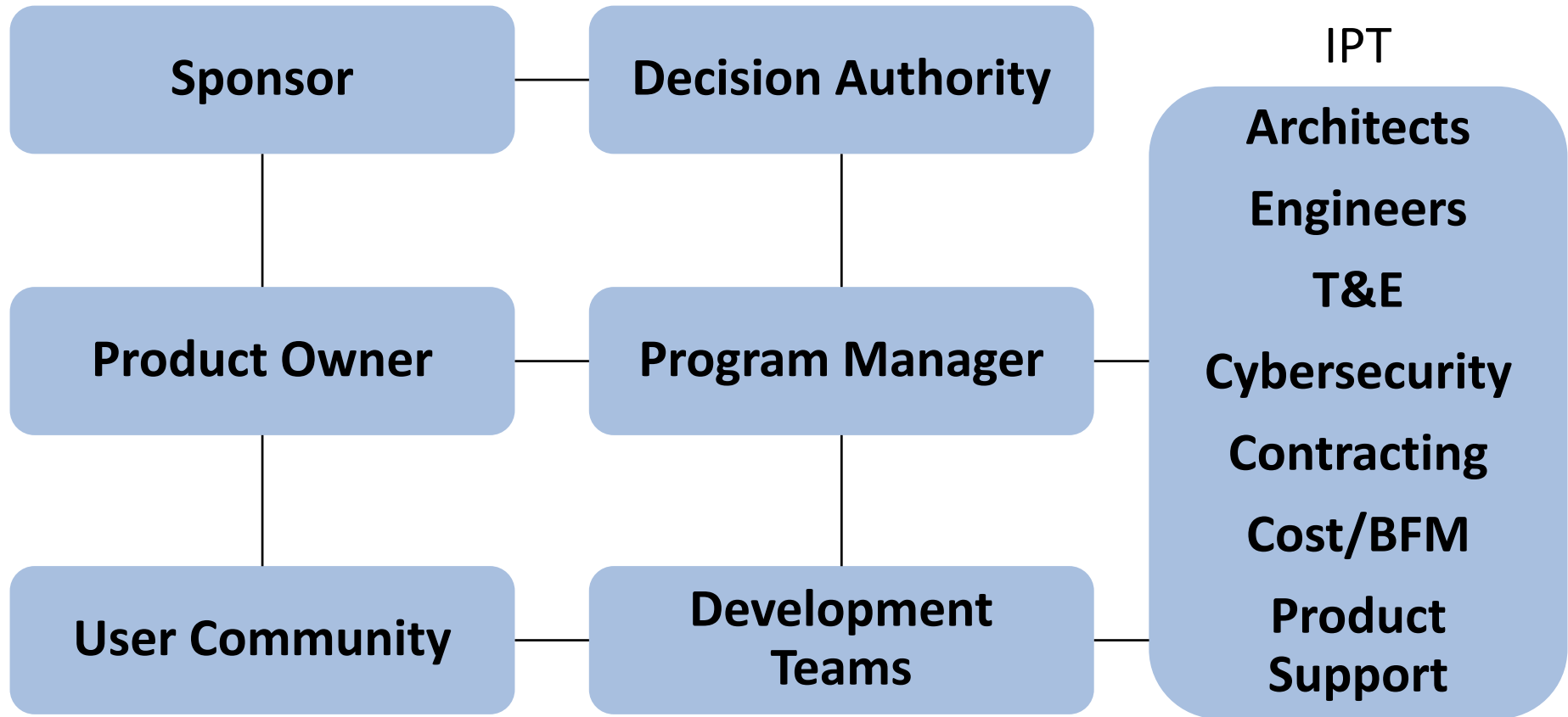
Rapid development and deployment of software running on commercial hardware (including modified hardware) and cloud computing platforms.

Embedded Software Path

Rapid development and insertion of upgrades and improvements for software embedded in weapon systems and other military-unique hardware systems.



Key Players in Software Acquisition Pathway



**Integrated Teams Across Operations and Acquisition;
Government and Vendors; All Functions and Levels**



Cyber Considerations Baked In Early

Fundamental principle: Cyber is to be addressed early and throughout the lifecycle using maximum possible automation; continually assessed and measured.

- Engineering resilience into the system
 - Development and tracking of a set of **metrics** to assess and manage the performance, progress, speed, **cybersecurity**, and quality of the software
 - Development of an **IP strategy** that supports cybersecurity and testing requirements
 - **Recurring assessment** of the supply chain, development environment, processes and tools

DevSecOps helps scale cyber & threat assessments: Automated and continuous monitoring of lower-level threats frees up effort for higher-level threats.



Cyber Considerations Baked In Early (2/2)

- Early and thorough DT&E to “Shift Left”; providing feedback to support “test, fix, and re-test”
 - Development of an **IP strategy** that supports cybersecurity and testing requirements
 - **Recurring assessment** of the supply chain, development environment, processes and tools
 - **Continuous and automated cybersecurity tests and cyber threat testing**, especially to support a continuous ATO or an accelerated accreditation process to the maximum extent practicable
- **Timely release** of software updates to address cybersecurity vulnerabilities; no less frequently than annually but potentially out-of-cycle based on criticality

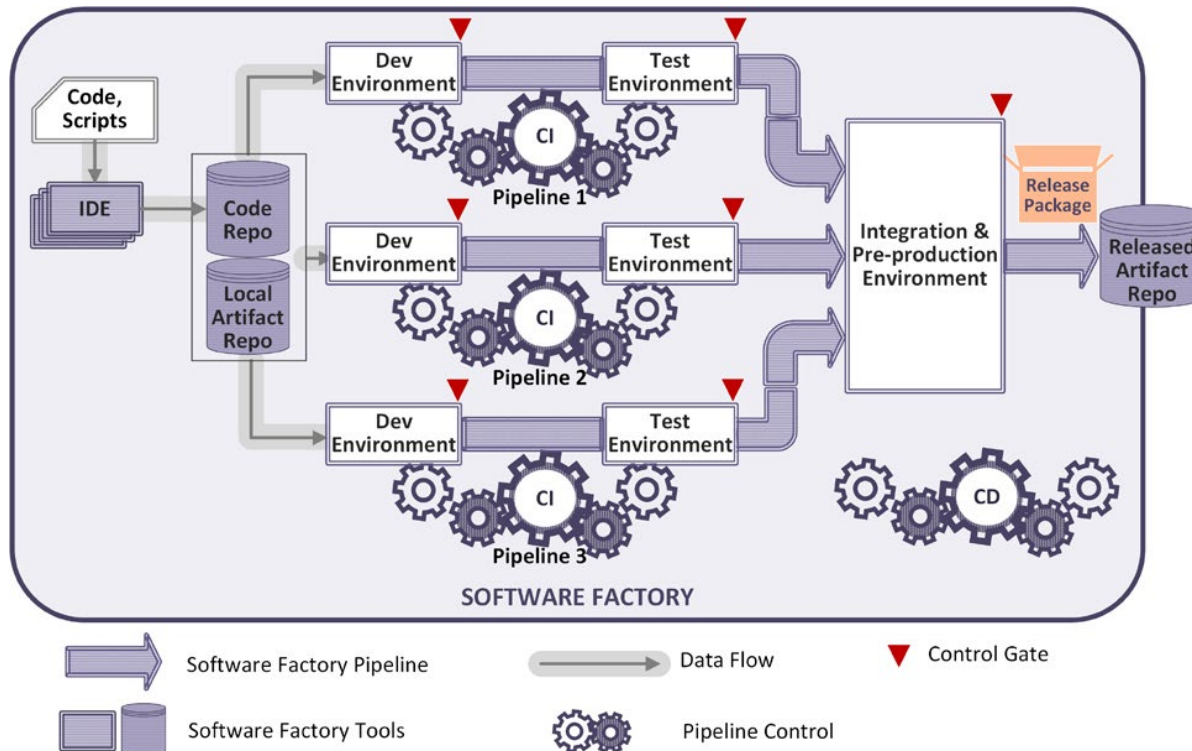
DevSecOps helps scale cyber & threat assessments: Automated and continuous monitoring of lower-level threats frees up effort for higher-level threats.



Plan For Enterprise Services and DevSecOps Pipeline (Software Factory)

People + Process + Tools = DSO Ecosystem

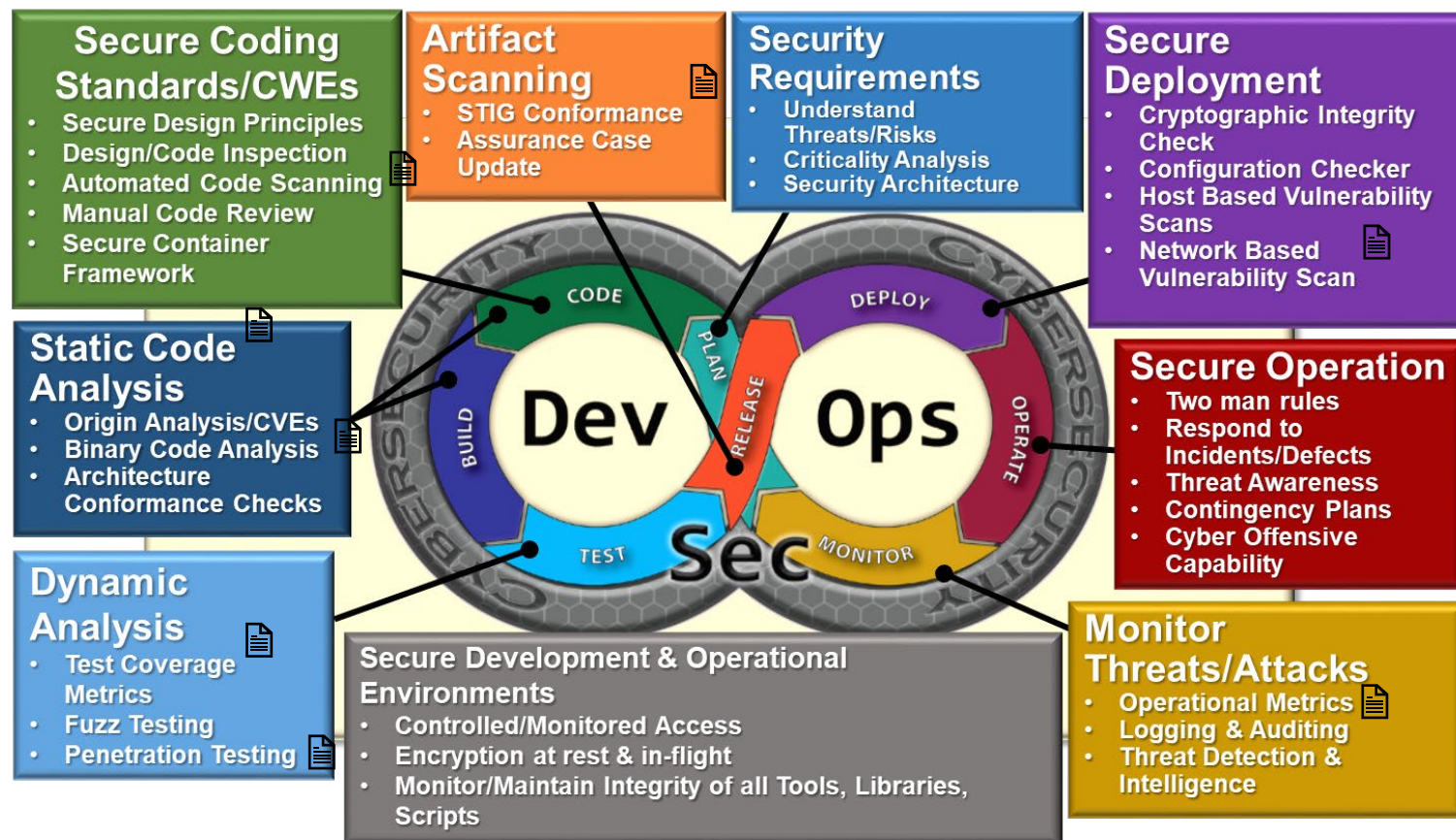
- Well-balanced Ecosystem & skilled workforce: path to DSO enlightenment
- Keystones:
 - Culture and Continuous improvement
 - Test Driven Development & Frequent Small Batch Delivery
 - Evolutionary Architecture **must** support frequent deliveries/interoperability
 - Refactoring and pay down technical debt





Secure Software & Cyber Security Plan

- The Sec in DevSecOps is baked into the planning, architecture and design, and embedded throughout the entire process
- DevSecOps **shifts Cybersecurity to the left**; true **risk managed** process
- Cybersecurity risk is continuously scanned, evaluated & monitored – yields **accessible, automated artifacts** enabling **continuous ATO**





Software Acquisition Pathway

Visit AAF website for integrated policy, guidance, and resources

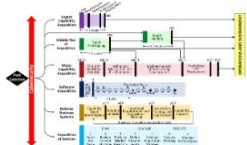


Home [Pathways](#) [Guidance](#) [Policies and Guides](#) [AAF Feedback](#) [Search](#)

SOFTWARE ACQUISITION

[AAF](#) > Software Acquisition

[Return to AAF Pathways](#)



Phases

[Planning Phase](#)

[Execution Phase](#)

Activities

[User Engagement](#)

[Design, Architecture](#)

[Test and Infrastructure](#)

[Program Management](#)

[Cost Estimation](#)

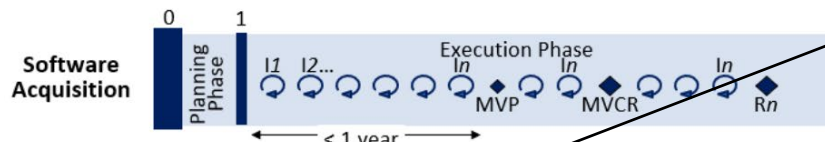
[Definitions and Glossary](#)

Software Acquisition

This pathway is to facilitate rapid and iterative delivery of software capability to the user.

[See what's changed recently.](#)

How to use this site



Tell us what you think. Please take a moment to [provide us feedback](#) on our site.

<https://aaf.dau.edu/aaf/software/>

Welcome your
inputs, feedback,
and questions.

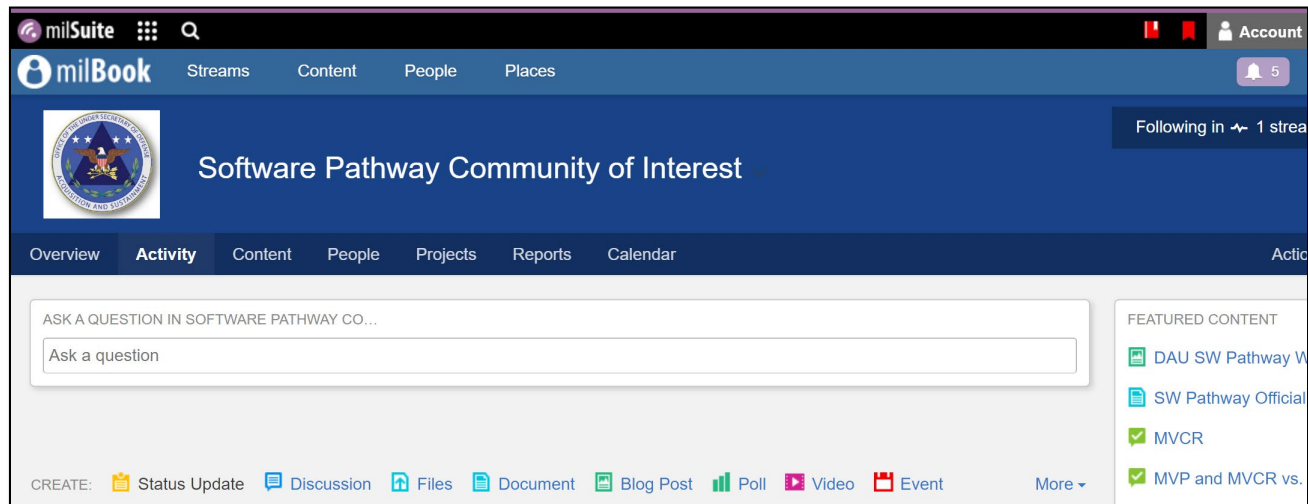
Adding FAQs and
new guidance soon.



SW Acquisition Pathway COI

Visit the Community of Interest to collaborate across the community on best practices, lessons learned, and draft templates

Ask questions here and we're also compiling FAQs

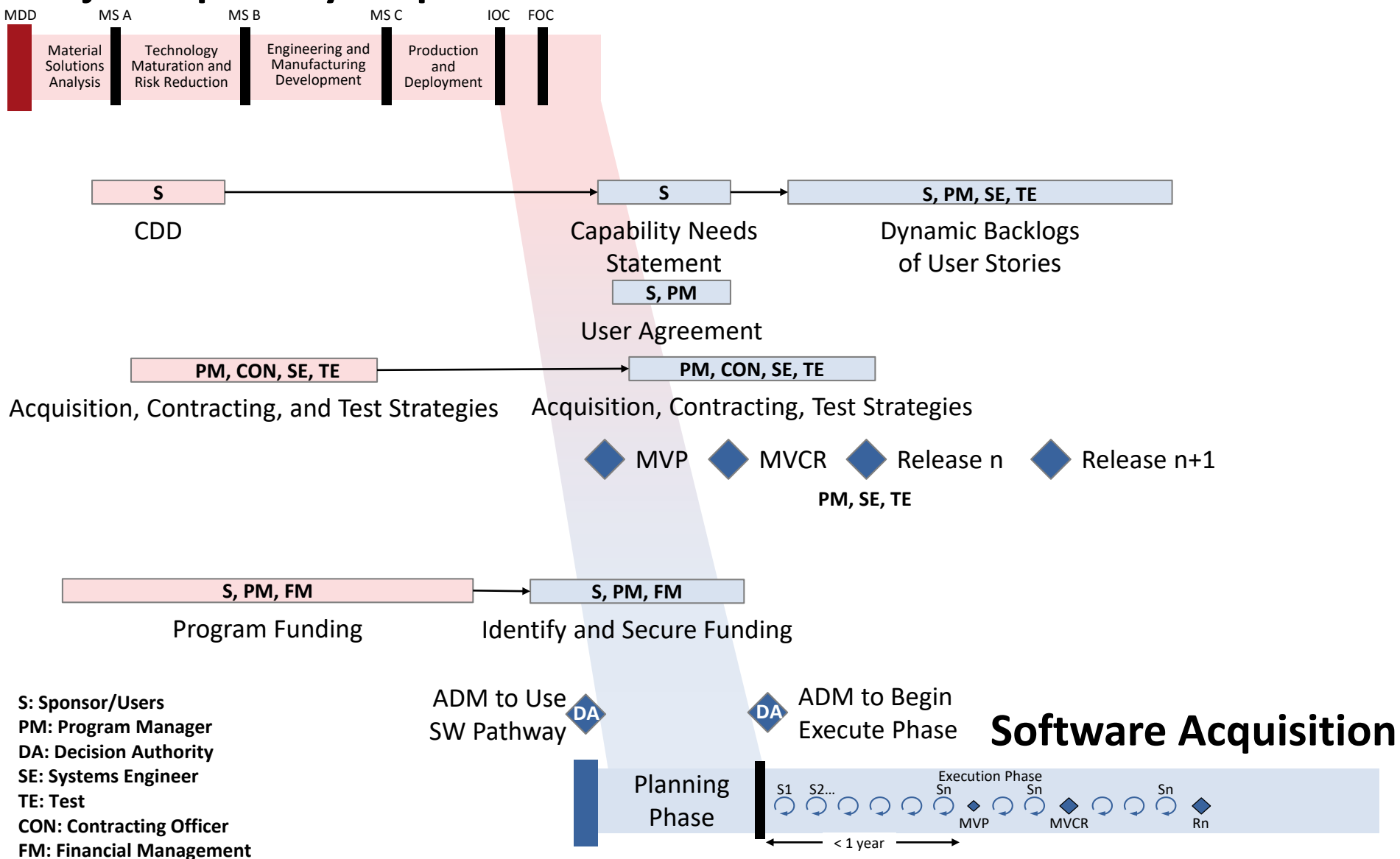


<https://www.milsuite.mil/book/groups/sw-pathway-community-of-interest> (Requires CAC)



1: Upgrading a Weapon System

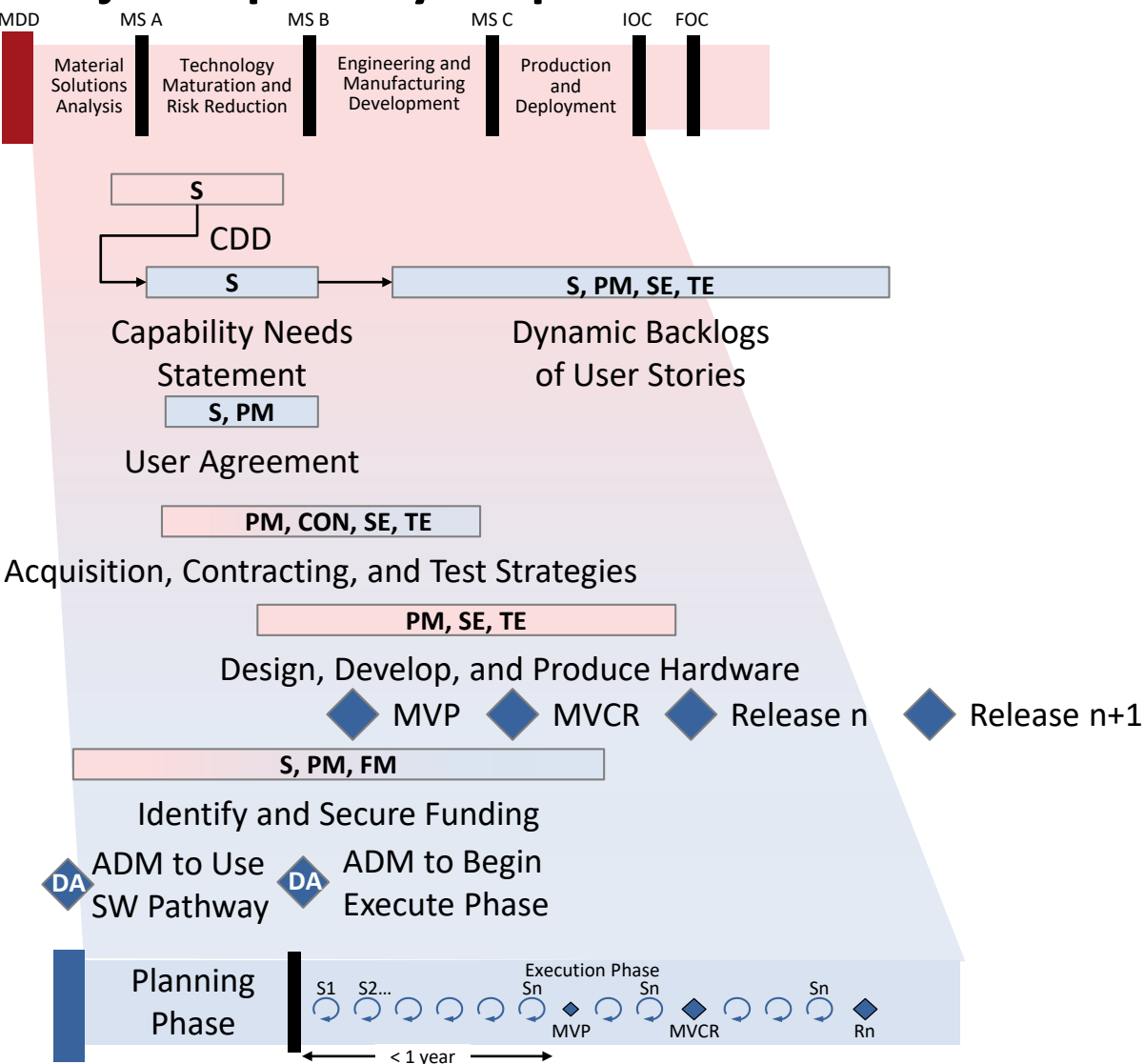
Major Capability Acquisition





4: Weapon System w/HW&SW Development

Major Capability Acquisition



S: Sponsor/Users
PM: Program Manager
DA: Decision Authority
SE: Systems Engineer
TE: Test
CON: Contracting Officer
FM: Financial Management

Software Acquisition