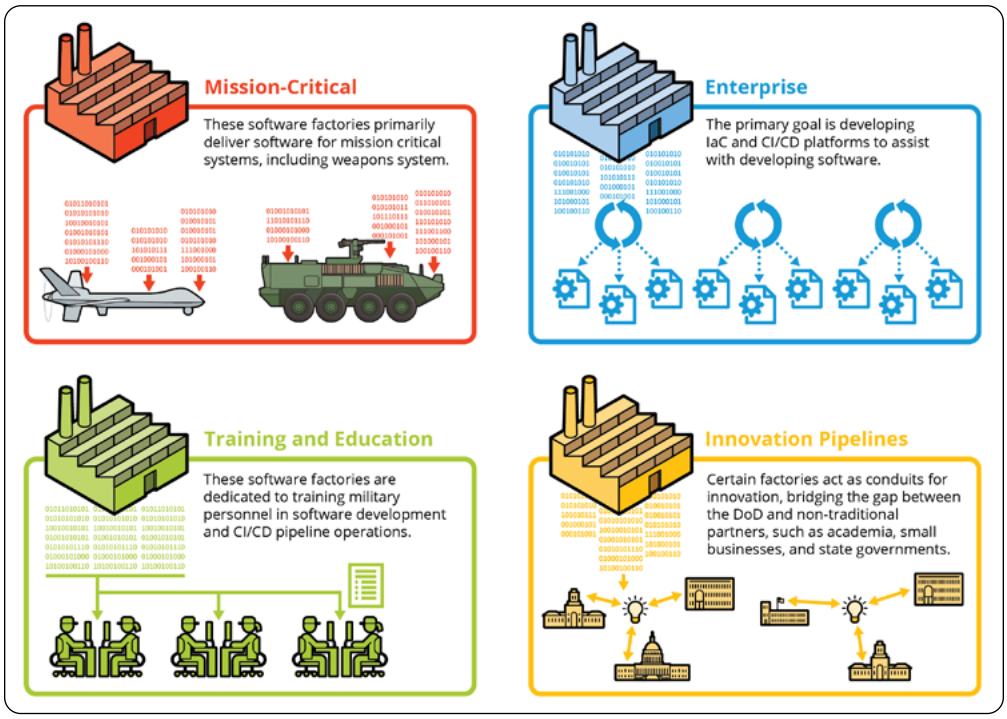
Carnegie Mellon University
Software Engineering Institute

The State of DevSecOps

In the last decade, DevSecOps approaches have taken foothold in the DoD. A proliferation of software development organizations and software factories now apply DevSecOps tooling and methods in programs across the DoD. The Office of the Chief Information Officer (CIO) is proud of the recent release of the State of DoD DevSecOps report which captures progress of DoD's goal to leverage DevSecOps to achieve faster delivery of software capabilities in support of Department priorities and increases information sharing across the DoD enterprise.

DoD has recognized that DevSecOps and the transformation of software development is crucial for mission success. We know this because industry has demonstrated the value of rapid software delivery into production. This brochure provides highlights from the report.

Software Factories: The Digital Arsenal for Modern Warfare



Each factory brings unique capabilities to the table, contributing to a broader ecosystem—a Digital Arsenal—that is more than the sum of its parts. This ecosystem is a testament to the innovative spirit within DoD—a spirit that thrives when given the freedom to evolve.

Mission-Critical: Some factories focus on delivering software for mission-critical systems, including weapon systems. These factories ensure that the software supporting our defense infrastructure is secure, reliable, and capable of adapting to evolving threats.

Enterprise: Some factories are building out IaC and configurable CI/CD pipelines to enable others within DoD to accelerate their transition to DevSecOps delivery, thereby, fostering a culture of continuous improvement and agility.

Training and Education: Other factories are dedicated to training military personnel in software development and continuous integration/continuous deployment (CI/CD) pipeline operations. As we recognize the importance of developers in the trenches, these efforts are building a more capable and resilient warfighting force.

Innovation Pipelines: Certain factories act as conduits for innovation, bridging the gap between DoD and nontraditional partners, such as academia, small businesses, and state governments. These factories play a crucial role in expanding DoD's talent pool and driving technological advancements from outside the traditional defense industry.

The conflicts in Ukraine demonstrate how quickly modern warfare is changing. The war started as cyber warfare, then moved to kinetic missile attacks on critical command and control as well as data centers, then to trench warfare, then to drone warfare, and now to electromagnetic warfare. All of these changes are happening in the modern battlespace, where the traditionally separate domains of air, land, sea, space, and cyberspace are merged in ways not previously imagined.

We need to make sure that DoD, as a warfighting force, has the IT resiliency and IT agility to adapt to those changes—in our weapons systems, command and control, intelligence, and battlefield prepping—faster than our adversaries.

As we move forward, DoD must embrace the entrepreneurial spirit of its software factories, expanding our Digital Arsenal to accelerate the transition to modern software development practices. This cultural transformation is crucial for leaving behind legacy waterfall methodologies and embracing the sense of urgency, collaboration, and continuous learning that successful DevSecOps requires.

SUCCESS STORIES

Air Force Launches New Software Directorate

In July 2023, the Air Force Materiel Command (AFMC), the Air Force's major command for defense systems acquisition, established a new Software Directorate within the Air Force Sustainment Center (AFSC/SW) to guide and integrate AFMC's software modernization efforts. The AFSC/SW has already completed an initial inventory and assessment of about 30 AFMC software activities, and it is already conducting a new round of assessments on its other software activities.

Department of the Navy Launches Software Factory Guidance

In early 2023, the Assistant Secretary of the Navy (ASN) Research, Development and Acquisition (RDA) and the Department of the Navy (DON) Chief Information Officer (CIO) released guidance to help the headquarters identify, understand, and optimize utilization of the Navy's software factory ecosystem and resources. The guidance included directions to register all DON software activities in preparation for a Service-wide software factory ecosystem review. The DON recently completed a Service-wide assessment all software factories and activities. The results will inform acquisition guidance and initiatives to optimize their software activities.

Army Establishes Acquisition and Governance Reform

In March 2021, the Headquarters, Department of the Army Chief Information Officer, (HQDA CIO) established the Enterprise Cloud Management Agency (ECMA), elevating it from an "Office" to a field operating agency. In March 2024, the Secretary of the Army issued Army Directive 2024-02, Enabling Modern Software Acquisition Practices, driving aggressive acquisition and governance reforms to help "rapidly develop, deliver, and adapt resilient software." The HQDA CIO is establishing a "Software Management and Response Team" (SMART) to provide a cadre of personnel with expertise and experience in modern software development practices. The Army also recently released a new Software Metrics and Management Policy that applies to virtually all of the Army's software-intensive programs.

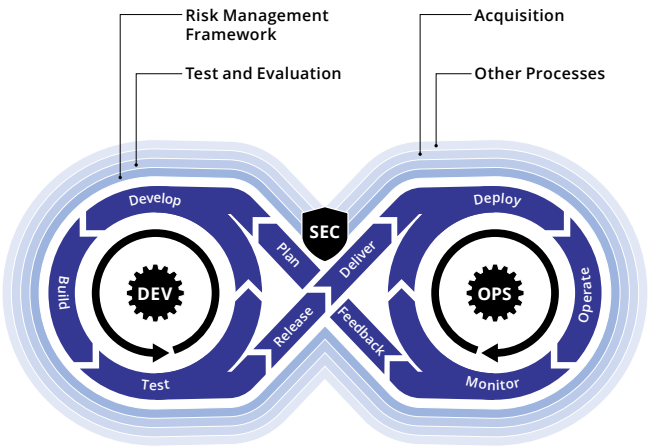
Third Time's the Charm for Software IT System Modernization

The United States Military Entrance Processing Command (USMEPCOM) is responsible for MIRS, a software system that tracks military applicants through their enlistment. The 1990's era application needed to be modernized to connect with new data sources and address cybersecurity and stability requirements. After two failed attempts using traditional approaches, MEPCOM had to adopt a new approach.

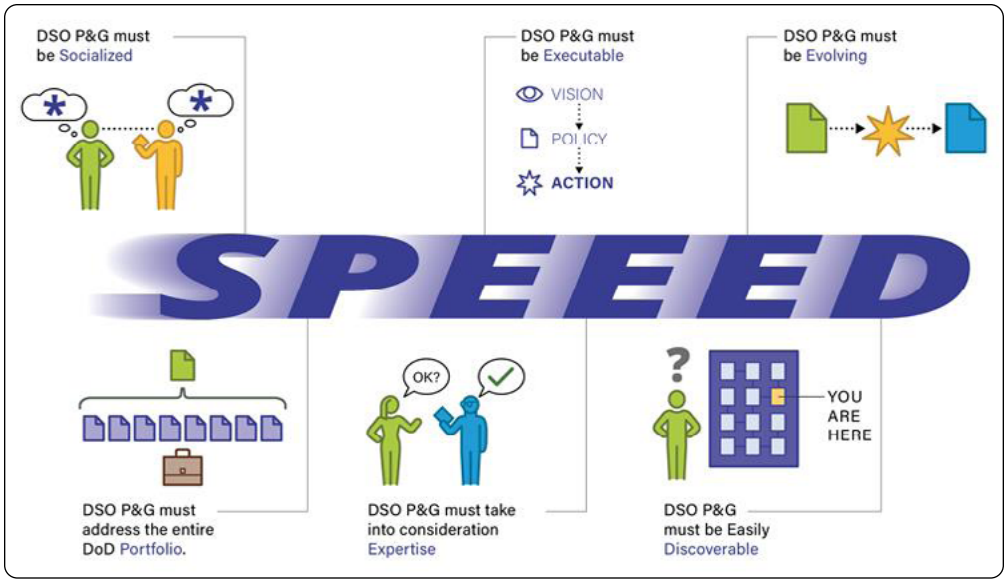
- Committed to using agile development and made modernization its top priority
- Leadership gave 51 percent authority in decision-making to the MEPCOM lead (Matt Lince)
- Built a team with the right skills
- Overcame cultural hurdles and policy barriers
- Collaborated with experts from other DoD software factories
- Changed the expectations of their user community and users now love the new process

Ultimately, the team's ability to innovate in the face of bureaucratic hurdles while changing cultural expectations led to their success.

Software Factory/Production Boundary



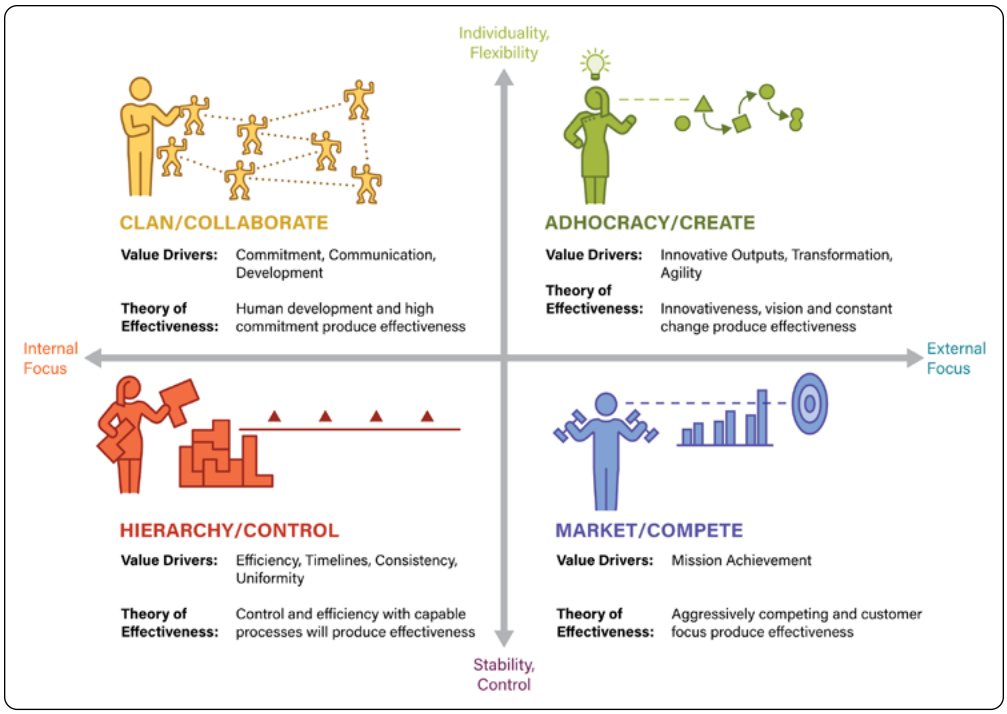
The Need for Speed



Study participants discussed the need for policy and guidance to keep pace with the rapidly changing technology and threat environment.

We identified six overarching characteristics for effective DevSecOps policy and guidance, summarized by the acronym S-P-E-E-E-D. Note that while these attributes were established in the context of DevSecOps, these principles apply equally to policy and guidance in any area characterized by the need for ongoing adaptation and comprehensive organizational change.

Competing Values Framework



The Competing Values Framework (CVF) is a model we can use for understanding, and ultimately aligning, organizational cultures.

DoD has embarked on a transition to modern software practices like DevSecOps to ensure that we consistently put the right capability in the hands of the right users at the right time, that it can be used effectively to accomplish the mission, and that it is adaptive to feedback in an ever-evolving landscape.

The success of DevSecOps within the DoD isn't just about technology—it's fundamentally about people: getting the right people in right place in the right roles.

Data Linking DevSecOps Organizations with Mission Outcomes

What do we want to understand?	How do we get the right data?
Did we build the right thing?	Seek evidence that the product is useful to the user: Does the product satisfy Measures of effectiveness (MOE) or other value metrics, defined by users?
Did we build the product right?	Look for evidence that the development process is stable, capability was built properly and will work properly. • Did we use DevSecOps effectively? • How did we implement security practices from requirements to deployment? • Did we employ the right build steps, checks, and tests? Have we managed quality? • Is quality stable over time? Have we removed cyber vulnerabilities? • Are we responsive to feedback from deployment and production? Measures may come from test reports, problem reports, change requests
Did we get the product to the right people?	Are the user roles clearly described? (Have they been documented, reviewed and validated?) Are the users qualified through training/certification/other means? (Has training been provided? Have the users been certified?)
Is the product delivered quickly and frequently?	Are we tracking lead times to user, and deployment frequency to operations or operationally representative environments? Are deployment frequencies stable/predictable over time? Measures may come from ticketing time stamps and release dates
Is the product delivered at the speed of relevance?	Measures should include lead times of business and technical processes that occur before coding starts or prior to release Measures may include lead time to qualified user, lead times for procurement/contracting, duration of certification activities
Is the product adaptable to change?	How long does it take to issue a fix or implement a change request or remediate a vulnerability? Measures may include time to repair, number of changes, time to implement changes from the ticketing system Are response times for critical fixes stable/reliable?
Is development responsive to user feedback?	Evidence should be found with change requests in the ticketing system properly labeled, prioritized, and tracked to successful closure

Using data to drive value

Data is a strategic asset. Data informs decision making at all levels of the organization. To maximize value, data should be defined, collected, and curated. When using data, some useful guidelines include the following:

> **The best data is the data used every day.** Operational data is used by the local organization to manage day-to-day business. This effort provides ongoing validation of its relevance and ensures it's up to date.

> **Manage to mission value, not metrics.** The metric is not the objective—it just tells you how you're doing against the mission objective. Use the metrics to guide toward the outcome. The focus is not just tracking technical metrics but understanding how they drive value for defense missions.

> **Don't rely on a single metric.** A single measure never tells the whole story. A variety of carefully chosen measures and metrics paints a complete picture. While the same data should be used to derive insight at all levels, neither the same metrics nor the same analyses are appropriate for all purposes.

> **Data can be aggregated, but metrics can't.** Metrics have already combined data, often in complicated ways. Don't combine again without carefully checking the math. Often, the metric used is a proxy, and not a direct measure.

Having the right workforce, with the right skills and information, in the right place, at the right time is critical to achieving our mission. When individual DoD software delivery organizations and their partners align to devise solutions that demonstrably improve local outcomes, they should capture and communicate these success stories and the supporting data through community forums, such as the Software Factory Coalition and the DevSecOps Community of Practice.

You can download the full report at:
https://dodcio.defense.gov/Library/

Please send your feedback to:
osd.mc-alex.dod-cio.mbx.devsecops@mail.mil