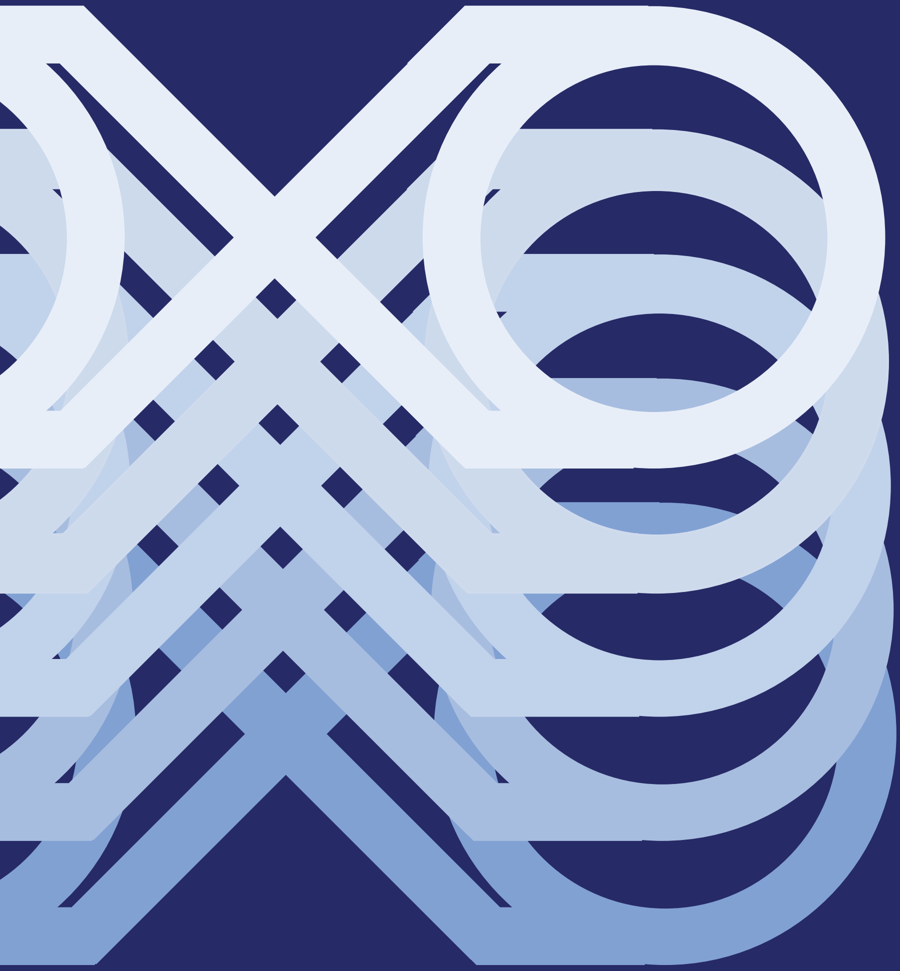
U.S. Department *of* Defense

The State of DevSecOps



March 2025

Distribution Statement A

Approved for public release: distribution is unlimited.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our readers, and don’t constitute or imply endorsement by the Department of any non-Federal entity, event, product, service, or enterprise.

Executive Summary

Since the release of the DIB SWAP report in 2019, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage,* the Department of Defense (DoD) has focused on transforming our software development and acquisition practices. The core of this transformation is DevSecOps, a process that breaks down silos, inculcates security, and rapidly delivers software into production following the best practices of modern technology companies. Over the past 5 years, DoD has made significant strides in adopting DevSecOps practices. There are over 50 software factories using DevSecOps to deliver code into production, learning how to incorporate these practices into the high-stakes DoD environment and providing templates and patterns for generalized transition.

Pockets of excellence have emerged across DoD in which DevSecOps practices have been successfully implemented, resulting in faster deployment cycles, enhanced security, higher software quality, greater operational efficiency, and improved end user value. This is why the Office of the DoD Chief Information Officer (CIO) is sponsoring this first "State of DoD DevSecOps Report" – to examine how far we have come, celebrate the wins, and gain insight to transition the entire Department to modern software practices.

DoD views DevSecOps as a critical enabler to protecting warfighters by driving modernization that adapts to future challenges and enhances overall mission success. DoD operates in a high-stakes environment where security, efficiency, and speed are paramount, and DevSecOps offers a pathway to achieve these objectives simultaneously. We know this because industry has demonstrated the value of rapid software delivery into production. Leading technology companies, commercial companies we hold in high regard, and even our adversaries are implementing this approach. DevSecOps enables DoD to continue to deliver advanced warfighting capabilities, such as Project Overmatch, the F-16, the F-35, and a broad range of other key weapons systems.

This study focused on the current state of DoD practices. We used quantitative metrics, although at this point in our journey, it was necessary to augment them with qualitative information via user surveys. Overall, the Department found that DevSecOps is a powerful tool for accelerating software delivery. When fully implemented, it changes the paradigm for delivering mission capability into warfighter hands at a speed that provides them with an asymmetric advantage.

DevSecOps is a process change that must be introduced with leadership commitment. To be successful it must overcome bureaucratic inertia aligned to traditional approaches that are intertwined across all facets of our delivery process. Figure 0-1 shows the DevSecOps infinity loop surrounded by traditional processes with existing equities that must be satisfied to deliver software into operations.

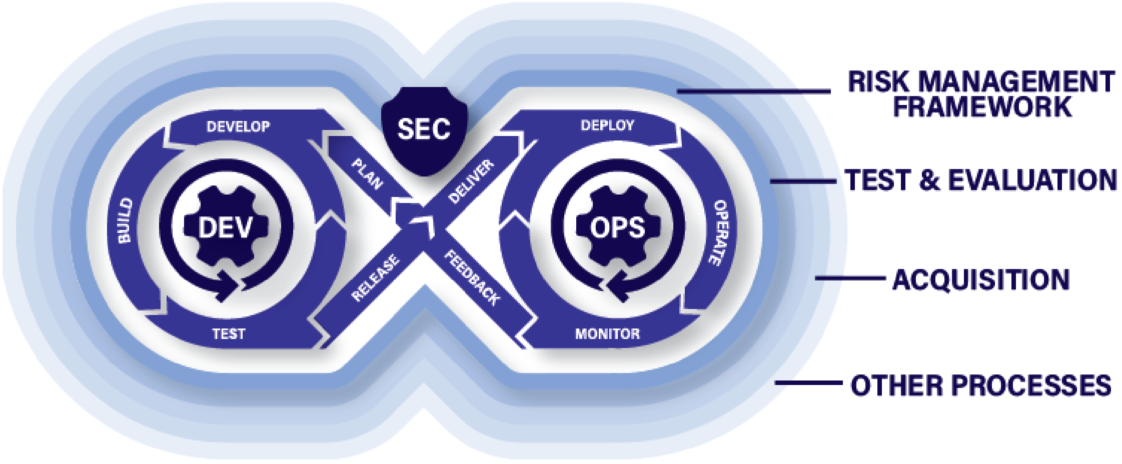


FIGURE 0-1: SOFTWARE FACTORY/PRODUCTION BOUNDARY

Existing Cyber practices, Test and Evaluation practices, Acquisition, and others including Requirements, AI, and Accounting all need to be realigned towards rapid, incremental delivery and operationalization of minimal mission capability. All of those authorities have proven capable of an agile transformation.

Over the course of the study, we interviewed more than 75 leaders and practitioners across DoD, representing 19 different software organizations of all types and test organizations representing Cyber, Developmental Test, and Operational Test. These leaders and practitioners demonstrated an impressive passion for the work and dedication to the mission. We encouraged them to share both their wins and opportunities for improvement. We used the insights we developed to present an approach for measuring and monitoring the progress of our transformation efforts and the health of our DevSecOps ecosystem as we move to the future. The following themes are expanded in the full report:

- **DevSecOps Achieves Success Amid Rapid Change**: DoD has made significant progress in adopting DevSecOps principles resulting in a more agile, resilient, and lethal force. DevSecOps validated the path forward by improving implementations, enhancing interoperability, and accelerating deployments.
- **Software Factories Are Our Digital Arsenal:** Software factories have revolutionized software delivery by applying continuous integration and continuous deployment workflows, and it’s time to scale and formalize their capabilities to modernize DoD’s IT and weapons systems environment. In DoD, a software factory is defined as a collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.
- **Software Factories Enable Modernization:** Expanding and optimizing the software factory ecosystem accelerates enterprise modernization. Software factories face challenges with consistent funding and business models that limit large scale expansion. DoD is collecting data, including costs and productivity, to inform future investments in people, processes, and technology and to drive more effective modernization.
- **DevSecOps Enables Continuous Authority to Operate:** DevSecOps enables a cybersecurity transformation from a point-in-time risk assessment to a continuous authorization to operate (cATO). cATO is a significant shift in DoD cybersecurity practices that incorporates real-time assessment, Zero Trust principles, and DevSecOps to secure our supply chain against emerging threats and improve our overall cybersecurity posture.
- **Policy and Guidance Enable Change:** Policy and guidance need to keep pace with the speed of software delivery enabled by DevSecOps and associated cultural changes to adopt new software. DoD is applying an agile mindset to drive policy based on grassroots success with DevSecOps. Examples of grassroots activities are the Software Factory Coalition and the DoD DevSecOps Community of Practice. Understanding cultural context enables DoD to deliberately align policy and guidance to effective practices.
- **Success Rests on Forging a Mission-Ready DevSecOps Workforce:** A skilled and motivated workforce is essential for DevSecOps, and DoD is making progress in building a robust workforce through initiatives like the Cyber Workforce Strategy Implementation Plan. Programs have reported that delivering capability into DoD mission is a significant incentive to drive recruiting and retention and can offset challenges of financial compensation. Effective leadership and a culture that prioritizes innovation, collaboration, and continuous learning are essential for fostering a workforce that can deliver DevSecOps capabilities at scale.
- **The Path Forward Relies on Data and Effective Measurement:** To ensure DevSecOps continues to enable mission value, DoD needs to measure progress against objectives, using data to inform decision-making, drive improvement, and remove barriers to progress. A combination of quantitative data, rigorous methodology, strategic thinking, and understanding of organizational goals is essential for effective decision-making.

The Office of the DoD CIO welcomes your feedback to improve the state of DevSecOps across the Department.

Table of Contents

1 Introduction: Studying the Current State of DevSecOps to Chart the Way Forward

DevSecOps is a cultural and technical movement aimed at fostering collaboration between development, security, and operations teams to build, test, and release software more rapidly and reliably. DevSecOps integrates critical security measures from the start, ensuring they're baked into the development process, not tacked on at the end. The newly revised "DoD Enterprise DevSecOps Fundamentals" states the following:

DevSecOps is a combination of software engineering methodologies, practices, and tools that unifies software development (Dev), security (Sec), and operations (Ops). It emphasizes collaboration across these disciplines, along with automation and continuous monitoring to support the delivery of secure, high-quality software. DevSecOps integrates security tools and practices into the development pipeline, emphasizes the automation of processes, and fosters a culture of shared responsibility for performance, security, and operational integrity throughout the entire software life cycle, from development to deployment and beyond.[1]

1.1 DevSecOps for Modernization and DoD Mission Success

DoD operates in a high-stakes environment where security, efficiency, and speed are paramount. DevSecOps offers a pathway to achieve these objectives simultaneously. DoD has its own specific needs and context, which don't always overlap and align with commercial software efforts.

The landscape of DevSecOps within DoD is undergoing significant transformation. This transformation extends beyond tools and technologies, encompassing culture, skillsets, processes, funding mechanisms, and inter-organizational dynamics. DoD has actively embraced DevSecOps by adopting a collaborative and agile approach to software development, thereby enhancing its software development practices.

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. Leading technology companies, commercial companies we hold in high regard, and even our adversaries are implementing this approach. DevSecOps enables DoD to continue to deliver advanced warfighting capabilities, such as Project Overmatch, the F-16, the F-35, and a broad range of other key weapons systems.

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. Since software increasingly enables almost all of these capabilities, DoD must not only continue implementing DevSecOps, recognizing and addressing the challenges and barriers, but also accelerate progress on this path.

1.2 The Need for a State of DevSecOps Study

The state of DevSecOps within DoD is evolving rapidly as we recognize its critical importance to our mission readiness and security posture. DoD has made significant strides in adopting DevSecOps practices, investing in recruiting and training, creating new work roles within the cyber and software communities, and integrating security into every stage of our software development life cycle. This transformation is driven by a need to deliver secure, resilient, and adaptable solutions in response

[1] DoD Chief Information Officer, "DoD Enterprise DevSecOps Fundamentals," Version 2, DoD October 23, 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Fundamentals%20v2.5.pdf.

to an increasingly complex threat landscape.

The Defense Innovation Board report, “Software Acquisition and Practices (SWAP) Study,” served as a critical trigger for this transformation, leading to the development and implementation of key policies and initiatives. Central to these efforts is DoD Instruction 5000.87, “Operation of the Software Acquisition Pathway,” which provides a comprehensive framework for agile, iterative software acquisition. Additionally, platforms and services such as Platform One, Iron Bank, and Big Bang have been instrumental in validating, standardizing, and securing our DevSecOps practices.

The Office of the DoD CIO has also provided foundational elements like DoD DevSecOps Reference Designs, which offer guidelines for integrating security into development, leveraging cloud-native technologies, and automating workflows. Other key initiatives include the DoD Cloud Computing Security Requirements Guide, the Container Platform Security Technical Implementation Guide, and the Cloud Native Access Point, which ensures secure access to cloud resources.

Pockets of excellence have emerged across various DoD organizations in which DevSecOps practices have been successfully implemented, resulting in faster deployment cycles, enhanced security, and greater operational efficiency. However, this journey isn’t without its challenges. DoD is actively addressing cultural resistance, skill gaps, and the complexities of integrating modern DevSecOps practices with our legacy systems.

DoD is committed to fostering a collaborative culture that prioritizes security and continuous improvement. By leveraging lessons learned from the private sector and investing in training and automated tools, we are building a robust DevSecOps ecosystem that supports our strategic objectives. While there is still work to be done, the progress we have made thus far is promising, and we are well on our way to achieving a fully integrated, agile, and secure set of DevSecOps environments across DoD.

The Office of the DoD CIO is sponsoring this first “State of DoD DevSecOps Report” to examine how far we’ve come, celebrate the wins, and gain insight to help plan our next steps.

1.3 Our Approach to this Study

Our approach to assessing the state of DevSecOps focused on high-priority aspects that provide insight into the overall transformation underway at DoD. Managing the portfolio of DevSecOps capabilities is not centralized, rather it is distributed across DoD Components. The state of portfolio management provides insight into the maturity and distribution of DevSecOps capabilities. Coordination across these distributed activities is the responsibility of the Software Modernization Senior Steering Group (SSG).

Over the past four years, both policy and general and detailed technical guidance have been published to move the software modernization forward. The impact and adoption of that policy and guidance provide insight into the overall state of DevSecOps and the effectiveness of advancing the transformation. Finally, the state of the DevSecOps workforce and culture provides insight into the ability of DoD to accelerate that transformation rate. We developed these priorities in a collaborative, cross-DoD workshop and organized the study along three lines of effort:

Portfolio Management

- How are DevSecOps activities aligned to mission and/or capability needs?
- How well do we understand the DevSecOps enterprise portfolio (people, process, and technology) from a DoD or Military Department-level perspective?

Policy and Guidance

- What policy or guidance changes have enabled DoD software entities under Software Modernization to improve the ability to deliver capabilities to the warfighter?
- What gaps or barriers exist in the current policies that prevent organizations from achieving the goal of speeding up capability delivery to the warfighter?

Workforce and Culture

- How conducive is the workforce and culture created by DoD and Military Departments to achieving the goals of DevSecOps?

In this first State of DevSecOps study, we worked to establish an initial quantitative baseline of progress on our ongoing DevSecOps transformation, then we worked to augment the quantitative data with qualitative insights. We collected the data to characterize our baseline progress in the following ways:

- We sought data from DoD and the Military Department-level inventories, assessments, and existing automated collection mechanisms.
- We met with practitioners a non-attribution basis to collect quantitative data about the implementation of technical and team practices associated with characteristics of healthy DevSecOps organizational cultures.
- We held workshops to map technical practices, processes, and implementations to related policy and guidance issues to identify accelerators, barriers, and gaps.
- We observed reporting from and engaged with practitioners in multiple DoD DevSecOps and software forums.
- We captured short success stories from members of the community that capture real experiences of teams on our journey.
- We leveraged insights developed from extensive bodies of work of two Federally Funded Research and Development Centers (FFRDC).
- We augmented these efforts with analysis of various DoD policy, guidance, strategies, and implementation plans, many of which have been issued during the course of our activities.

Over the course of the study, we interviewed more than 75 leaders and practitioners across DoD, representing 19 different software organizations of all types and test organizations representing cyber, developmental, and operational test. These leaders and practitioners demonstrated an impressive passion for the work and dedication to the mission. That passion and dedication to the mission encouraged everyone we talked with to share both their wins and opportunities for improvement. We used the insights developed to present an approach for measuring and monitoring the progress of our transformation efforts and the health of our DevSecOps ecosystem as we move to the future.

Describing the data strictly along these lines of effort independently misses important interdependencies. We can't describe the culture and workforce independently of the mission and organizational structure. The effectiveness of policy and its implementation depends upon the workforce culture and the specific mission. Policy is always interpreted through the lens of culture. The existing portfolio and policies affect how the workforce is built.

The Office of the DoD CIO welcomes your feedback on the ways in which you have used this report to understand and address ongoing DevSecOps challenges, and any other feedback or information that could improve the state of DevSecOps across DoD.

1.4 A Reader's Guide to this Report

Here's a quick navigation guide and section summary to help you get the most out of this report:

Section 2: We celebrate wins along the journey all across DoD – and there are many of them! This section also features (with permission) the story of the MEPCOM Integrated Resource System modernization. It is an inspiring software modernization success story that touches on every aspect of our transformation: innovation, creativity, tools and technologies, culture, skillsets, processes, funding mechanisms, and inter-organizational dynamics.

Section 3: DoD's software factory innovation ecosystem grew up organically. In this section, we set the stage by highlighting the evolution and entrepreneurial nature of DoD's software factory ecosystem, the importance of effectively equipping our thriving Digital Arsenal, and the need to maintain its highly collaborative culture to accelerate the transition to modern software development practices.

Section 4: Acquisition program managers and enterprise IT leaders will gain new insights from important efforts underway to establish a clear enterprise inventory of DoD's software factory and DevSecOps portfolio, and the complexities in the funding and business environments that drive the need for strategic governance to enable optimization of the software factory ecosystem.

Section 5: Continuous ATO (cATO) represents a significant shift in the management of cybersecurity risk from point-in-time to continuous risk management. This section highlights ongoing efforts between DoD CIO and DoD Components to provide resources that support this transformation.

Section 6: Transformational leadership is required to help everyone "get to yes." In this section, we discuss developing policy and guidance at all levels in a way that enables the cultural shift across DoD toward a DevSecOps mindset.

Section 7: Software team leads, stop here! DoD is working on comprehensive strategic initiatives aimed at building a robust DevSecOps workforce. This section takes the pulse of leaders in software teams and provides updates on important strategic initiatives underway to address challenges in recruiting, retention, and workforce development.

Section 8: Pull this section out to build action plans. It offers goal-oriented guidance for collecting and using data to gain continuous insight into progress toward strategic objectives, to identify and understand barriers and challenges, and to adapt rapidly and responsibly to changes in our ever-evolving landscape. We discuss data as a strategic asset and ways in which it can be captured to explicitly link DevSecOps organizations with mission outcomes.

Section 9: This handy reference section contains a list of all public sources cited and consulted.

Throughout this report, important information is highlighted in various ways:

- Key takeaways for each report section appear in blue sidebars at the beginning of each section.
- Quotes from leadership and key quotes from the report text are presented in green sidebars.
- Success stories appear in sections in the body of the section in which they appear.

2 Celebrating Successes So Far

Five years have passed since the Defense Innovation Board issued its SWAP report, and in that period, DoD has tallied numerous accomplishments and successes. The Office of the Secretary of Defense (OSD) has laid a solid foundation for DevSecOps development based on industry guidance, and many pockets of excellence have been established across various DoD organizations. These have included a combination of significant initiatives as well as smaller, fast-moving efforts, showing that it’s possible to implement DevSecOps and demonstrate how DoD as a whole should move forward.

There are many indications of progress. For instance, the Iron Bank container repository has experienced an explosion of new containers and now holds over 1,200 hardened container images with approximately 400 commercial and 800 open-source images. In addition, the repository has launched a new Core Image Program to help focus resources on maintaining the most critical and highest utilized images across its user base. The Military Department CIOs have issued continuing guidance and updates to implement these practices and accelerate adoption. Perhaps most importantly, however, many programs have adopted the Software Acquisition Pathway (SWP). The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) has been collecting data on the growing number of programs adopting DoDI 5000.87. At present, approximately 78 DoD acquisition programs have adopted the software acquisition pathway. Seventy-five percent of those programs are delivering software in less than six months.[2]

DoD has made substantial progress on our DevSecOps journey, and change is happening fast.

A combination of significant strategic initiatives and smaller, fast-moving efforts continue to demonstrate successful DevSecOps implementations and point the way forward for the DoD.

In its most recent Weapon Systems Annual Assessment, the Government Accountability Office (GAO) reported that 75 to 80 percent of the 40 Major Defense Acquisition Programs (MDAP) it monitors have adopted modern development practices, including Agile and DevSecOps.[3] GAO found that almost half of those MDAPs deliver software capability in less than four months.

DoD Components, Program Executive Offices, Programs of Record, and even the defense industrial base have taken the SWAP report’s guidance to heart and have begun to implement and use that guidance to deliver using modern practices. We’ve highlighted below a few Military Service-level efforts and an inspiring vignette from a program on its software modernization journey. Look for many more success stories in subsequent sections.

We are moving quickly – this section captures only a small number of the stories and indicators of progress along DoD’s DevSecOps transformation journey.

[2] Department of Defense. “Structuring Change to Last: An Update on Innovation at the Department of Defense.” U.S. Department of Defense. August 2024. https://media.defense.gov/2024/Aug/07/2003519333/-1/-1/0/DoD-INNOVATION-FACT-SHEET-AUGUST-2024.PD

[3] Government Accountability Office. “Weapon Systems Annual Assessment: DoD Is Not Yet Well-Positioned to Field Systems with Speed.” GAO-24-106831. Government Accountability Office. June 17, 2024. https://www.gao.gov/products/gao-24-106831

Throughout the remaining sections of this report, you'll see additional success stories called out in highlighted sections below.

Success Story: 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.[4] 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.[5][6]

> This retooling of our AFMC software factories is a perfect example of an enterprise solution that's laser focused on the warfighter... We're expecting this consolidation will allow seamless integration of other AFMC software factories in the future and serve as a model for software development in other major commands.
>
> *— GEN Duke Z. Richardson, AFMC Commander*

Success Story: 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.

> [W]e're seeing technological breakthroughs that are redefining conflict. The Navy recognizes that speed matters... that the pace at which we procure, modernize, maintain, and sustain our platforms matters... as does the pace at which we rapidly integrate and adopt new technologies.
>
> *— ADM Lisa Franchetti, Chief of Naval Operations*

Success Story: 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. The flagship Army Software Factory (ASWF) has been part of this ecosystem. 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."[7] 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.[8]

> These reforms will enable the Army's adoption of best practices for software development and accelerate the Army's digital transformation to deliver needed capabilities to Soldiers.
>
> *– HON. Christine E. Wormuth, Secretary of the Army*

[4] Robertson, Corey. "New software organization to foster collaboration." Air Force Sustainment Center Public Affairs. July 7, 2023. https://www.aflcmc.af.mil/NEWS/Article-Display/Article/3452478/new-software-organization-to-foster-collaboration/

[5] AFSC Software Directorate's Public Home Page: https://afscsoftware.dso.mil/

[6] Gen Richardson quote in sidebar: Robertson, Corey. "New software organization to foster collaboration." Air Force Sustainment Center Public Affairs. July 7, 2023.

[7] Cloud.Mil. "What is DevSecOps?" U.S. Department of Defense Cloud.Mil website. September 27, 2024 [accessed]. https://www.cloud.mil/devsecops/

[8] U.S. Army. "Army Directive 2024-02, Enabling Modern Software Development and Acquisition Practices." March 11, 2024. U.S. Army Publishing Directorate. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN40433-ARMY_DIR_2024-02-000-WEB-1.pdf

Success Story: 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.

The organization committed to using agile development and made modernization its top priority. Senior leadership chose Matt Lince to lead the effort and gave him the authority to make key decisions. They drafted a charter, signed by the Commander and Senior Executive Service leader, which established a standalone team to develop the new system. With unwavering leadership support, the project was deemed a "no-fail" operation. Leadership gave Matt 51 percent authority in decision-making, allowing him to make the hard decisions and ensuring disagreement would be resolved quickly. No single person could veto or "non-concur," the team effectively abandoned the necessity to achieve full consensus.

Matt formed a dedicated team of 20-25 government personnel, chosen from across the organization to ensure multidisciplinary representation. He divided the team into sub-teams with carefully selected leads, emphasizing the need for collaboration and mutual support. To expand the team's capabilities, they brought in a nontraditional contract vendor, doubling the team's size and creating hybrid teams with overlapping government and contractor personnel.

Matt identifies hiring as one of the top challenges transitioning to DevSecOps within DoD. He faced resistance from traditional experts who were hesitant to adopt innovative staffing practices. However, through education and cultural shift, they accepted new ideas. Matt's approach to hiring starts with inspiring candidates with the mission and showcasing the impact they can make, then offering competitive incentives, flexible schedules, modern technology, and opportunities for skill growth. He also moves quickly to hire top talent and retain the best people before they're scooped up by other opportunities.

The team faced significant structural and cultural hurdles in meeting their strict delivery deadline, including DoD and Service-level policy and bureaucracy, as well as internal resistance to changes in business processes and longstanding barriers. This pushback was intense during the first six months, but the team also gained key allies and change agents. Additionally, they struggled to procure necessary tools in a timely manner, but persistence and creative problem-solving helped them find ways around these obstacles. For example, they discovered that many policies were more restrictive than DoD or Service-level regulations, so they worked with senior officials at the Pentagon to find ways to navigate these policy barriers. By building relationships with officials, they could identify areas that allowed for more flexibility. They also got ideas from other DoD software factories about new ways to meet business needs. Indeed, they were pleasantly surprised at how many internal business functionals embraced these new ways of overcoming obstacles, and they started to apply them to other challenges in the organization.

The final challenge the team had to overcome was changing the expectations of the user community. Previous attempts to modernize the system used a waterfall development process, which was, at least, partially to blame for their failures. This time, the command embraced the agile approach to consistently deliver a minimum viable product (MVP)—building only what was strictly necessary to accomplish the core mission, with no extras. This initially received substantial pushback from their users, who had never had systems delivered with missing "nice to have" functionality and imperfections. Matt and the team prioritized fixing the key "pain points" for users ahead of adding features after initial deployment. Every two weeks the team delivered working software to the user community that incrementally improved the system and fixed issues. Their first goal was to improve the users' "quality of life" and after a few months users found that the system wasn't so bad. The system continued to improve in subsequent months, as missing features—and then new features—were gradually delivered. As users became used to the MVP concept, they didn't complain when the next MVP system came out, because they knew it would quickly improve. Gradually, the users came to love the new process and culture change took root. Ultimately, the team's ability to innovate in the face of bureaucratic hurdles while changing cultural expectations led to their success.

3 Software Factories Constitute the Digital Arsenal for Modern Warfare

DoD defines a software factory as “a collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.”[9] In the evolving landscape of DoD, software factories have emerged as a vital and dynamic force for modernization. Far from being mere assembly lines, these factories are hubs of innovation, driven by entrepreneurial spirit and a deep commitment to enhancing DoD’s capabilities. They represent a grassroots movement that has grown organically to meet the urgent needs of modern warfare and defense.

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.

DoD’s current software factory portfolio emerged organically as individuals and programs recognized the need to adopt commercial best practices to meet emerging defense priorities. As they have transitioned from nascent capability to delivering DoD capability, they have had to overcome challenges finding the right business models to survive within the Department. In the absence of a strategic centralized approach, every successful software factory had to evolve its own business operations. Most efforts have been successful but were accomplished through perseverance and dedication.

The Challenge: Updating and Scaling the Digital Arsenal

Formalizing, maturing, and scaling software factories is an imperative for achieving and sustaining modern defense capabilities. Software factories address several needs:

- Enabling highly-automated deployment of code and configuration.
- Enabling repeatable processes for rapidly deploying, and re-deploying, high quality and secure code into production.
- Ensuring robust operations and continuous monitoring of fielded systems to detect anomalies, enhance resilience, and rapidly respond to emerging threats.
- Most important: systematically equipping DoD with the “software weaponry” needed to maintain strategic advantages against adversaries in a digital world.

It hasn’t been easy to adopt modern software practices at the pace and scale needed to enable modern defense capabilities. The scattered use of legacy practices has stubbornly impeded progress in some cases. Over the past four years, it has become apparent that DoD needs to apply more consistency to nurturing and managing the software factory ecosystem. The MILDEPs are becoming more proactive in this effort, which should produce faster growth and adoption of software factories having common funding and acquisition models, common workforce management, and streamlined access to enterprise service portfolio offerings.

DoD intends to have the MILDEPs and DISA manage the software factory ecosystem portfolio and optimize for DoD Components’ unique missions. The Office of the DoD CIO is planning to write DoD policy to codify successful, evidence-based practices and to strengthen the Digital Arsenal.

Software factories have revolutionized software delivery in the DoD.

Individual leaders and teams have championed innovation to rapidly meet emerging defense priorities.

It’s time to take software factory innovations to the next level.

Grassroots successes now need formal support extend and scale the capabilities of our software factory ecosystem to modernize an increasing portion of the DoD IT and weapon systems environment.

One size doesn’t fit all.

Distinct categories of software factories have emerged to serve a variety of mission needs, reflecting the multifaceted needs of the DoD. They behave differently, and cultural differences between them reflect their different mission priorities.

[9] Cloud.Mil. “What is DevSecOps?” U.S. Department of Defense Cloud.Mil website. September 27, 2024 [accessed]. https://www.cloud.mil/devsecops/

Success Story: The Software Factory Coalition

The Software Factory Coalition (SWFC) champions the innovation of our software factories by bringing together their diverse perspectives to "improve innovation by sharing discoveries, swarm to solve problems, and self-govern software factory functions to enable reuse, reduce unnecessary duplication, and allow for necessary specialization."

This grassroots community holds monthly virtual meetings, quarterly in-person meetings, conferences, symposiums, and an annual summit at which they share experiences, problems, and potential solutions in a safe environment. The meetings bring together the factories, industry representatives, and key policy and decision makers. For more information on the SWFC, visit https://coalition.dso.mil.

3.1 Understanding Software Factories

At their core, software factories are collections of people, tools, and processes designed to continuously deliver software that meets the specific needs of end users. These software factories leverage automation to replace manual processes, allowing for rapid iteration, enhanced security, and greater alignment with mission objectives. However, not all software factories are created equal; they serve a variety of missions, reflecting the multifaceted needs of DoD.

Mission-Critical Platforms: 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.

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.

Infrastructure as Code (IaC) and CI/CD: 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.

3.2 Support, Not Control

Concern exists within the DevSecOps community that the typical DoD approach to governance—rooted in hierarchy and control—may stifle this emerging ecosystem. Rather than assuming some correct number of software factories exists, we should place our focus on outcomes: How many of our systems are leveraging DevSecOps and agile practices to deliver mission-critical capabilities? How many are still trapped in legacy, waterfall models that can't keep pace with the changing environment? How can we extend the capabilities of the DoD software factory ecosystem to modernize an increasing portion of the DoD IT and weapons systems environment?

Our focus should shift to how we can grow and extend the capabilities of our software factory ecosystem: How does the Department effectively support and encourage the ongoing collaboration and self-optimization that's happening organically within the software factory ecosystem? By providing them the necessary resources and support, we can accelerate the transition of more DoD IT infrastructure to modern, agile, and DevSecOps approaches. Doing so will not only enhance operational readiness but also ensure that our defense systems remain adaptable and resilient in the face of evolving threats.

3.3 Understanding DoD's DevSecOps Culture

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.

In the following section, we'll explain how we used the behaviors and practices in DevSecOps organizations to measure culture and share what we learned when we interviewed personnel at three different kinds of software factories.

Understanding culture requires analysis of artifacts and practices in context. Those artifacts and practices reflect the shared understanding that guides behaviors (a team might refer to this as "how we do business"). To talk about culture in DevSecOps teams in a meaningful and repeatable way, we needed to develop an objective, evidence-based approach. We derived seven major DevSecOps cultural attributes from industry and academic literature, and the extensive experience of the Software Engineering Institute[10] and MITRE Corporation.

7 DevSecOps Cultural Attributes

Leadership: evidenced by clear vision, tools and resources, a supportive environment and the removal of barriers.

Effective Communication: includes behaviors that exhibit common language and effective sharing of information, including goals, risks, tasks, commitments, and strategies.

Collaborative Team Environment: characterized by shared responsibility and cooperation toward common goals.

Empowered Workforce: demonstrated by self-organization, problem solving, and continuous improvement.

Rapid Feedback Loops: includes behaviors that demonstrate open dialogue with peers and users, and the use of constructive feedback to improve processes and outcomes.

Continuous Learning and Skill Development: evidenced by policies and behaviors that demonstrate both the availability and use of learning resources and skills-development programs.

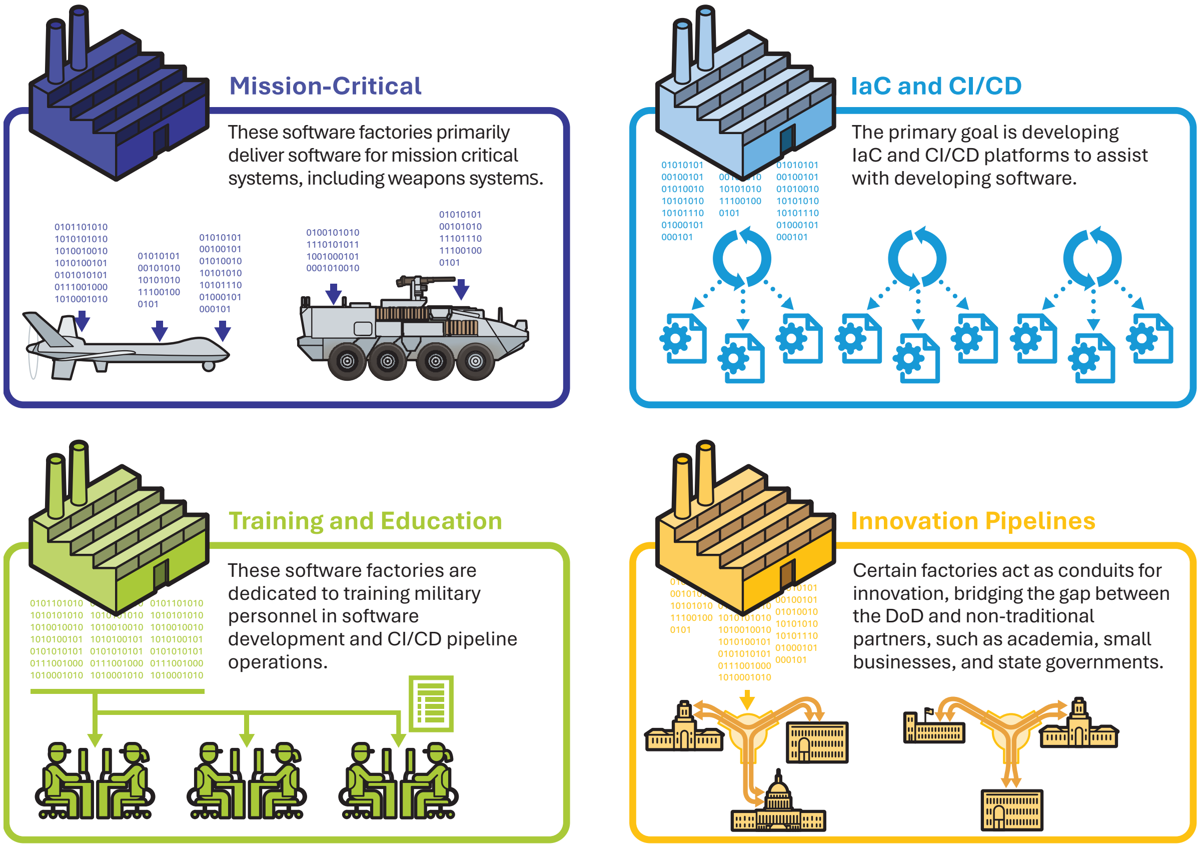
Skilled Workforce: indicated by alignment of team skillsets to the requirements of current and future projects.

We used an established DevSecOps readiness assessment (which has been implemented with over two dozen DoD DevSecOps organizations) to derive 41 questions on team practices across these seven categories. We also established a rubric practitioners used to objectively rank the availability, frequency, degree, etc., of these artifacts and practices in their organization. Higher scores indicate use of more and better practices associated with that category. We also asked about use of metrics, reporting of metrics, and process measures including deployment frequency and lead times.   In addition, we asked practitioners to provide concrete examples of artifacts or process descriptions.

To limit the disruption to software teams, we did not attempt a comprehensive survey with a broad data call. Instead, we attempted to find a representative sample that would provide an initial indicator and validate the approach. The Office of the DoD CIO provided contacts from the Software Factory Coalition and assisted with introductions. Over the course of several months, we met with 36 practitioners from 19 software organizations across the DoD Components. Each of the individuals we met with identified themselves as being from one of the categories of software

[10] The Software Engineering Institute is funded and supported by OUSD(R&E) under Contract No. FA8702-15-D-0002 with Carnegie Mellon University.

Software Factories: The Digital Arsenal for Modern Warfare



Mission-Critical

These software factories primarily deliver software for mission critical systems, including weapons systems.

IaC and CI/CD

The primary goal is developing IaC and CI/CD platforms to assist with developing software.

Training and Education

These software factories are dedicated to training military personnel in software development and CI/CD pipeline operations.

Innovation Pipelines

Certain factories act as conduits for innovation, bridging the gap between the DoD and non-traditional partners, such as academia, small businesses, and state governments.

FIGURE 3-1: SOFTWARE FACTORIES ARE FAR MORE THAN JUST ASSEMBLY LINES

factories illustrated in Figure 3-1 below.[11] The different types of software factories not only have different missions and value propositions, but we also found that they stressed different aspects of DevSecOps culture.

Figure 3-2 shows the average scores on the seven cultural aspects for each software factory type. The scores represent the degree to which factory behaviors, as reported by respondents, aligned with the cultural attribute. The highest-ranking attribute differed for each factory type. The ordering

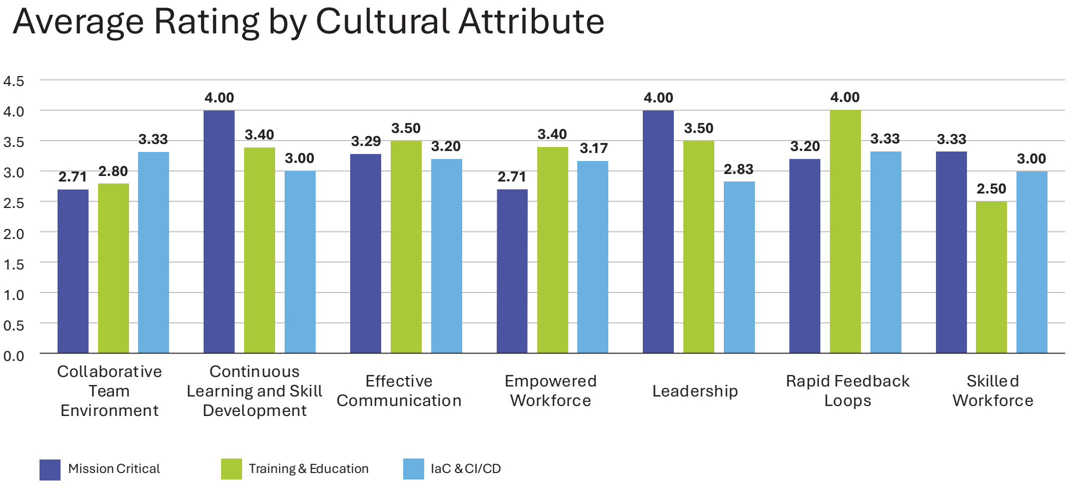


FIGURE 3-2: BEHAVIOR PROFILE CULTURAL ATTRIBUTE CATEGORY

[11] A participant from the Innovation Pipelines category was not available for this study. Future studies will be sure to include this group.

does not appear random but instead reflects both the software factory mission and what is needed to overcome those challenges.

Our overall responses and analysis indicated how the behaviors vary between the different categories of software factories, and that this variance appears to align with their mission type. It seems that the most strongly developed behaviors are aligned with cultural attributes that reflect mission priorities.

In the next few subsections, we'll discuss the cultural attributes that are most highly developed for each of these three types of software factories.

Mission-Critical Software Factories

In Mission-Critical software factories, the observed behaviors suggested that "Leadership" was the highest developed attribute. From this observation, we concluded that in the early stage of transformation, continuously developing, integrating, and fielding software requires strong leadership for mission success. In Mission-Critical software factories, leadership needs to ensure the stakeholders are communicating and barriers to progress are removed. Leadership often makes difficult judgment calls to prioritize action over full consensus. For example, see the MEPCOM success story in Section 2, in which the lead could exercise a "51-percent vote."

Training and Education Software Factories

The mission of Education and Training software factories is to arm individuals with DevSecOps and agile skills they can take back to their projects to share and apply. (Some of our participants referred to these organizations as "Incubators.") For example, the XVII Airborne Data Warfare Center (DWC) was staffed with many graduates of the TRON development program. Incubators have a human-centric culture that assumes a lower level of skill among the staff, which shows in the rankings in the Skilled Workforce area. Given the focus on training service members for deployment to Mission-Critical Software Factories, it isn't surprising that the most strongly emphasized behaviors in these organizations were associated with the "Continuous Learning and Skill Development" and "Rapid Feedback Loops" categories. Interviewees understood the importance of these behaviors to enable rapid delivery of mission capabilities. For example, they mentioned "[it's the] point of the program," and there were "days where we've done [deployments] 20 times."

Infrastructure as Code (IaC) and CI/CD Software Factories

The IaC and Managed CI/CD Pipelines software factory organization's value proposition is to create and configure a highly integrated software development environment and tool stacks to make software development as efficient as possible while maintaining cybersecurity and quality practices. These practices reflect how an IaC and Managed CI/CD Pipelines software factory facilitates software development flow and removes inefficiencies across environments used for the software development life cycle (e.g. development, test, integration, staging, production). The four cultural attributes with the most strongly developed practices include "Continuous Learning/Skill Development," "Collaborative Team Environment," "Effective Communication," and "Rapid Feedback Loops." Because creating and evolving a software pipeline requires frequent communication among team members and a broad range of customers, it isn't surprising these behaviors were well developed. Likewise, rapid feedback is essential to satisfy the user base.

Platform One exemplifies a practice demonstrating effective communications and rapid feedback. It not only has a Customer Experience Officer with technical and business account managers tracking customer experience but also enables end users to communicate directly with developers.

Baseline and Moving Forward

DoD's software factory ecosystem arose largely as the result of grass-roots innovation and leadership to solve specific, local mission challenges. Four distinct types of software factories emerged organically to satisfy the different needs of those missions. In turn, the supporting software development organizations place different emphasis on how aspects of DevSecOps culture support their mission. This study validates that they are indeed distinct types with distinct needs. These different contexts have different implications on funding/budgeting, business models, infrastructure, and workforce needs – and different measures of success. Our goal is to nurture our software factory ecosystem by scaling proven, effective practices in relevant mission contexts:

keeping in mind that one size doesn't fit all.

We have provided a baseline for measuring the degree to which behaviors that align with cultural attributes associated with DevSecOps are present in DoD software factories. We can use this baseline to observe how behaviors mature over time and potentially correlate these with outcomes including delivery speed, workforce retention, and user satisfaction. Understanding the moderate cultural divergence across the factory types helps us not only to understand the different needs of the different types, but it can also help us better diagnose their cultural health in the future.

Future information gathering could include the following activities:

- Surveys based upon the interview questions delivered quarterly or twice a year would enable a frequent health check, identification of trends, and an evaluation of how other changes affect the culture.
- Conducting workshops to examine the culture directly with practitioners could provide a way to triangulate with other measures of change management.
- Instrumentation of practices could enable the gathering of objective data on areas such as use of formal training and workforce skills.

DoD's software factory ecosystem must continue to evolve in response to internal learnings, external technologies, and mission needs. Continuous improvement requires collaboration, rapid feedback loops, and continuous learning and skill development, all attributes of a healthy DevSecOps culture. It is through continuous improvement that we ensure our defense systems remain agile, resilient, and capable of meeting the evolving challenges of tomorrow, ultimately strengthening our ability to protect freedom and democracy while avoiding unnecessary conflicts.

4 Optimizing the Software Factory Ecosystem Enables Enterprise Software Modernization

The DoD Software Modernization Implementation Plan released in 2023 established a task to "optimize and increase adoption of the software factory ecosystem" and called on DoD to "inventory digital platforms and software factories." DoD's expansive software factory landscape largely stems from organic, grassroots innovation efforts. DoD's next evolutionary step is to transition these organic efforts to the management of software factories as DoD Component-essential assets, where capabilities, projected workload, resources, and scalability become routine considerations in their DoD Components' mission and investment planning:

- Conducting an initial, comprehensive ecosystem inventory of DoD's software factories, including their technical capabilities and capacity, their operational sponsor/user communities, and currently supported missions. This inventory will help DoD focus its available resources and drive programs to the right factory (or factories) per their operational needs and schedules.
- Establishing and implementing automation to help DoD Components and OSD more quickly collect, update, and share basic inventory and status information.

This section highlights challenges and solutions that have emerged across the Department in pursuit of the optimization of the Digital Arsenal.

4.1 Inventorying the DevSecOps Software Factory Portfolio

DoD Components have been conducting extensive data call/survey activities to inventory their software activities and fully classify their ecosystems. These efforts collect data on the motivation for establishing the activity, mission, capabilities, tools, infrastructure, staffing, technical and business processes, funding support, and more. The data forms a benchmark to qualitatively baseline and prioritize the progress of strategies relative to the defined optimization measures among of the software factory ecosystem.

These troves of data can be used to assess the mission alignment of their software factories, software development capacity, and the costs of delivering capability, thereby enabling the development of DoD Component-level governance strategies. Analysis of this data and regular monitoring of ecosystem health and mission alignment will enable identification of opportunities to further extend the capabilities of the software factory ecosystem and take an outcome-focused approach to establishing strategic, enterprise portfolios of software factories across a broad, well-understood range of technical requirements.

DoD remains committed to identifying opportunities where efficiencies and infrastructure redundancies can be consolidated. However, we must ensure that the pursuit of efficiency does not overly constrain our ability to choose the most

Information is power when making software ecosystem investments.

DoD is improving the collection and automation of the software factory portfolio and cost data necessary for making the right investments in people, processes, and technology to meet mission needs and adapt to new challenges.

Appropriate funding and business models are necessary to ensure mission outcomes.

Software factories today employ widely different funding and staffing models, often combined in novel and complex ways to meet diverse mission objectives. The DoD is collecting data to understand which business models most effectively support different software factory mission environments.

appropriate technical solutions for unique contexts or our ability to invest in innovative efforts to solve new problems and adapt to meet changing mission imperatives.

Establishing an enterprise-level characterization of the software factory portfolio will be a powerful instrument for the whole of DoD in understanding overall DevSecOps adoption and effectiveness in advancing its software modernization goals. As we discussed in Section 3, this understanding is crucial to making the investment decisions (in people, process, and technology) necessary to transition more and more of DoD's software capacity out of inadequate legacy approaches. It will also improve our insight into the effectiveness of business processes associated with software factories in different contexts, cost, and capacity modeling for effective resourcing and more.

Success Story: The Air Force Sustainment Center's New Software Directorate

The Air Force Sustainment Center Software Directorate (AFSC/SW) is already using data from its extensive enterprise inventory effort to realign the Air Force Material Command (AFMC) software factories around specific software production missions and improve idea sharing. The mission-oriented alignment will "prioritize the delivery of software while expanding agility and innovation," and leaders expect it to enable seamless integration of future AFMC software factories. The realignment will also consolidate some software activities to reduce duplication of effort across AFSC's Software Engineering Groups. To learn more about this effort, visit https://afscsoftware.dso.mil.

4.2 Improving and Automating Inventory Data Collection

Currently, there are several systems, approaches, and reporting cycles for collecting DevSecOps metrics from the DoD Components and acquisition programs. Acquisition programs currently provide various subsets of their DevSecOps metrics or status information to multiple OSD stakeholders, often by differing means, formats, or reporting systems. Multiple initiatives are underway to leverage automation and federated data management to streamline and simplify data collection efforts and improve analytical capabilities. Two of the mandatory reporting systems are the Defense Acquisition Visibility Environment (DAVE) and the DoD IT Portfolio Repository (DITPR).

DAVE, owned by OUSD(A&S), collects programmatic metrics on acquisition programs, including SWP programs which report SWP-required metrics semiannually. (SWP-required metrics track key DevSecOps metrics to provide insight into the health of the acquisition pathway, and not for program oversight/control.) The DAVE team coordinates with acquisition program management offices (PMOs) on a case-by-case basis to build application programming interfaces (APIs) to obtain a program's data based on the technical capabilities of the acquisition PMO. The Advana platform operated by the DoD Chief Digital and Artificial Intelligence Office (CDAO) offers comprehensive reporting and visualization on many SWP program metrics.

DITPR, owned by the DoD CIO, is the Department's central, authoritative inventory of unclassified, mission-critical, and mission-essential IT systems and their interfaces. DITPR has a web-based, form-driven user interface for data entry that includes the capability to upload additional IT program inventory files as required. One of the DoD CIO's goals is to establish an authoritative, automatically updated catalog of software factories and DevSecOps platforms, spanning defense mission areas.

The DoD CIO Cloud and Software Modernization (CSM) Directorate is coordinating with OUSD(A&S) on a pilot effort to develop an API for DITPR to leverage the visualization and reporting features in the Advana platform to make it easier to analyze DevSecOps data collected in DITPR.[12]

[12] For more info about Advana, see the DoD Chief Data and AI Officer's Advana 101 Briefing Book (May 2024). https://www.acq.osd.mil/asda/dpc/ce/p2p/docs/training-presentations/2024/p2p%202024%20-%20procurement%20analytics%20data%20in%20advana%20part%20i.pdf

4.3 Managing the Software Factory Portfolio

Software factories across DoD evolved around local mission needs, rather than being strategically aligned with the multiple Department-level mission objectives. The leaders of these grass roots organizations had to develop business models for funding and staffing their operations using their own resources and conforming to program-level policy. Consequently, there are a wide variety of approaches in use across the entire ecosystem. Over the past year, significant effort has been applied across the Military Departments to better align and manage their software factory capabilities, as we discussed in Section 2:

- Air Force Sustainment Center (AFSC) Software Directorate
- DON SWF Report and Optimization Strategy for the Ecosystem
- Army CIO's Reorganization and Issuance of Army Directive 2024-02, "Enabling Modern Software Development and Acquisition Practices"

Members of the software factory ecosystem community frequently discussed a need to approach DoD software factories and pipelines as customer-driven products, rather than as mandated solutions. A customer focus drives the effectiveness of management activities to consolidate and optimize the software factory portfolio. Some interviewees felt that DoD tries to force consolidation instead of building services people want to use. Ultimately, DoD's management policies are influenced by many factors, including guidance and mandates from Congress, the White House Office of Management and Budget, and other federal authorities.

While several study participants understood the benefits of potential consolidation (e.g., potential cost efficiencies, streamlined training, and infrastructure management practices), some also felt that consolidation will only work when a much broader range of technical requirements is understood and codified to address as part of a strategic, enterprise portfolio of software factories. Participants expressed concern that the initial enthusiasm to promote DevSecOps and associated software factories downplayed some of the technical complexities that differentiate systems and drive their pipeline requirements. That concern influences some programs to create their own pipelines and/or software factories because large "enterprise" software factories don't support their unique needs. DoD and Military Departments, on the other hand, have concerns about the costs of duplicative capability.

Funding and Acquisition Complexity

Most DoD software factories were launched like startup companies, with a home organization that provided, effectively, seed funding to launch them. In industry, tech startups are expected to grow their profit margins and become less reliant on venture funding rounds as their revenue can be used to operate and grow the business. The path for our DoD software factories is not as clear. The home organization may be able to continue to provide some level of centralized funding support, or ongoing operations need to be funded by various customers or program elements.

In the next few subsections, we'll discuss how balancing needs for continuity and adaptability, serving a wide variety of software factory "customers" and mission needs, and structural challenges in the DoD budgeting process have led to the proliferation of myriad different funding and business models across the Digital Arsenal. There's no one-size-fits-all model but establishing an effective business model to support a specific software factory's mission is critical to realizing mission value.

Needs to Balance Centralized versus Decentralized Funding

Practical needs dictate a combination of both centralized funding and cost recovery to operate a software factory or software delivery organization. Some level of "steady state" operations is needed to ensure the availability and continuity of core expertise and workload capacity. There will also be novel, unpredictable situations—including urgent operational customers' needs and new security threats—driving the need for short-notice augmentation of DevSecOps expertise or infrastructures. Centralized funding is also not without complexities: a RAND study of Air Force software factories in 2022 indicated that Kessel Run received funding from at least five different program elements, and that while Kobayashi Maru was receiving program-element funding from the Joint Space Operational

Center Mission System (JMS), it was not sufficient to meet the software factory's funding and personnel needs.[13]

DoD has many different mechanisms to fund programs and projects, varying across different DoD levels, DoD Components, and priorities. Generally speaking, software factory funding sources can be described as centralized or fee-for-service. Table 4-1 offers just a few examples of software factories using various types of funding mechanisms.

Funding Types	Description	Example
Fee for Service (where a customer program provides funding based on the services they use)	Working Capital / Cost Recovery	SKI CAMP; DISA C2
	Enterprise Capabilities for Purchase	TRMC; CSSP; Platform One
	Services (app development, workforce development, etc)	TRON; Army Software Factory; BESPIN
Centralized Funding Model	POM / Direct Appropriation	Platform One
	Acquisition Models/Program Elements	Kobayashi Maru; Kessel Run
	Funding from a Higher Headquarters Organization	BESPIN; Corsair Ranch

TABLE 4-1: TYPES OF SOFTWARE FACTORY FUNDING

Table 4-1 isn't intended to offer an exhaustive list of the funding mechanisms used by any single software delivery organization. Data previously gathered by DoD CIO indicate that many organizations have established combinations of centralized and fee-for-service funding models.

The Air Force's Business and Enterprise Systems Product Innovation team (BESPIN), for example, receives centralized funding from the Air Force PEO BES, in addition to funding from customer organizations. Kessel Run (the first Air Force software factory, launched in 2017), a unit within DAF PEO C3BM, receives funding from acquisition program elements and from customer programs throughout the Air Force. Tron received a significant amount of its funding through Small Business Innovation Research (SBIR) programs.

Who Are the Customers?

Software factory customers are derived from a vast range of organizations with disparate funding channels. Software factory users may come from elsewhere in the DoD, as well as other government and non-governmental entities. For example, the U.S. Space Force regularly invoices non-government entities for launch, support, and custom development services. Several Air Force software factories are both mission-specific instantiations and customers of Platform One. Software factories including BESPIN, Tron, and Rogue One have received funding through partnerships with small businesses on SBIRs. The Digital Transformation Office partnered with the Digital Platform as a Service Office out of the Air Force Life Cycle Management Center/HNII (AFLCMC/HNII) to create LaunchPad, an environment built on top of Cloud One, delivering digital-engineering-related software solutions to over 650 users from 175 different organizations. Acquisition across organizations in a single DoD Component, between DoD Components, and involving entities from outside the DoD and government will all have unique funding, security, visibility, and intellectual property rights.

Budget Challenges

The DoD's typical budget justification processes (e.g., long lead times for advance planning) make it very challenging to make "fee-for-service" cost recovery models work in the DoD. Many people we interviewed observed that the Program Objective Memorandum (POM) and the Planning, Programming, Budgeting, and Execution (PPBE) processes aren't geared to support budget planning relative to the value delivered by software factories. Restrictions on mixing different funding appropriations for RDT&E (3600), O&M (3400), and Procurement (3080) create significant administrative hurdles, but doing so is almost a requirement due to the blended nature

[13] Keller, K. M.; Lytell, M.C.; & Bharadwaj, S. "Personnel Needs for Department of the Air Force Digital Talent: A Case Study of Software Factories." RAND website. March 30, 2022. https://www.rand.org/pubs/research_reports/RRA550-1.html

of development and operations inherent in delivering modern software. The purchasing of software licenses creates uncertainty regarding the allowed use of RDT&E versus O&M funding in the first year versus subsequent years of use. The cumulative effect of policies such as separate funding for software development and maintenance constrains the agility needed for DevSecOps.

Exploring the Use of Single Appropriation for Software

The disconnect between the appropriation structure and effective software development practices has been long recognized. The Budget Activity-08 (BA-08) pilot program, established by Congress in FY21, authorized realignment of existing appropriations to enable a set of pilot programs to execute all software activities under RDT&E, to enable the DoD to study the effects of the approach.[14] The Space C2 software factory ("Kobayashi Maru") is one of the authorized pilot programs.[15]

Thus far, BA-08 programs "have reported more frequent and improved technical deliveries over time. This is because single appropriation funding is immediately available upon a real and timely need, with the benefit of avoiding program and budget cycle requirements to change color of funding from RDT&E to procurement" and additional programs have been added to the pilot since.[16]

In 2023, the PPBE Reform Commission chartered by Congress under the FY22 NDAA "demonstrated the value of reducing color of money barriers for software"[17] and issued a recommendation to "Allow Procurement, RDT&E, or O&M to be Used for the Full Cycle of Software Development, Acquisition, and Sustainment."[18] While this is certainly an exciting validation of the hoped-for benefits of a single-appropriation approach, the BA-08 pilot programs remain underway to continue to report to Congress on the effects. This spring, the Army released its new software acquisition policy, under which program offices scheduled to transition in FY24 or later, will no longer transition to a sustainment phase, and instead continuing to operate under RDT&E funding.

Mission Risk of Ineffective Business Models

Several DoD software factories indicated they have inadequate business models to support the level of effort and growth they are expected to achieve. While some factory leaders bristled at being held to long-term budgets in a dynamic environment, DoD Components noted that the software factories can't yet adequately model use of funds. The consequence of inadequate business models keeps those software factories underfunded and understaffed, which can affect both morale and the timely delivery of capabilities. When the early assumptions underlying a software factory business model are overcome by events, programs can incur significant unexpected costs. In a cost-shared funding model, if the forecasted number of participating programs falls short, early adopters can wind up with a significantly heftier bill.[19]

Complicating matters, cloud services have been purchased through a wide variety of contracts with differing terms and utilization data isn't captured or reported in uniform ways, contributing to the difficulty in calculating and forecasting true costs in fee-for-service approaches. The Joint Warfighting Cloud Capability (JWCC) Indefinite Delivery, Indefinite Quantity (IDIQ) contract is addressing cloud acquisitions through a multi-cloud vehicle available across DoD. The MILDEPs and DISA are establishing cloud service offices that leverage JWCC and provide consistent guidance and policy for accessing cloud resources.

[14] Office of the Under Secretary of Defense for Acquisition and Sustainment. "Budget Activity (BA) 'BA-08': Software and Digital Technology Pilot Program Frequently Asked Questions." U.S. Department of Defense. September 28, 2020. https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Budget%20Activity%20-%20BA-08.pdf

[15] Bianco, Jessica and Laura Hujber. "Measure and Assess the Effectiveness of Navy and DoD Pilot BA-08 (software) Program Performance." Naval Postgraduate School website [accessed October 1, 2024]. https://dair.nps.edu/bitstream/123456789/4948/1/SYM-AM-23-176.pdf (Accessed 2024-08-16)

[16] Ibid.

[17] The Congressional budget defines different categories of funds and their specific uses.

[18] U.S. Senate Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform. "Recommendations for Inclusion in the Appropriations Bill or National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2025." Commission on PPBE Reform website. October 1, 2024 [accessed]. https://ppbereform.senate.gov/wp-content/uploads/2024/04/ConsolidatedLegLanguageforFY25_Final.pdf

[19] Ineffective Cost Modeling sidebar citation: Keller, K.M.; Lytell, M.C.; & Bharadwaj, S. "Personnel Needs for Department of the Air Force Digital Talent: A Case Study of Software Factories." RAND website. March 30, 2022. https://www.rand.org/pubs/research_reports/RRA550-1.html

Ineffective cost modeling can lead to (or worsen) negative acquisition and resource management outcomes, including the following:

- “Mission creep” due to feeling a need to pursue funding opportunities elsewhere.
- Understaffing, leading to failures to deliver capability in a timely manner.
- Unnecessary spending.
- Redundant investments.
- Unintended competition among software factories.

4.4 Managing the Software Factory Workforce

Most software factories employ a mix of military, DoD civilian, and contractor staff adding complexity to workforce management. (In this section we will discuss challenges and opportunities associated with growing and maintaining the DoD software engineering workforce.) From prior 2022-2023 software factory survey responses and our discussions with some software factories this year, we learned how some of them are augmenting their staff or services to cover their internal and customer needs. A large software factory in one of the defense agencies is leveraging IDIQ approaches. Separately, one of the Services’ large software factories mentioned recent positive experiences using Other Transaction Authority (OTA) agreements. Platform One used basic ordering agreements (BOAs) to acquire qualified contractors to build, secure, and sustain DevSecOps platforms. Other innovative contracting mechanisms are being evaluated and implemented throughout the DoD to support platform development teams, onboarding teams, product development teams, cybersecurity teams, and IT operations. (We discuss DoD’s workforce development initiatives in Section 7.)

We don’t currently have insight into how widely IDIQs or OTAs are being used in the DoD to enable DevSecOps activities. However, this is an area the DoD Components could closely monitor to capitalize on efficiencies (e.g., for proportionally sharing contract costs and consolidating similar requirements to negotiate more favorable vendor rates).

4.5 Acquiring Software Factory Services

Many people we interviewed described challenges they faced acquiring software factory services. It’s important to consider that these acquisition processes, while owned by many different entities, are an important part of the overall software factory ecosystem. They affect speed of software delivery but may be invisible in technical software tracking metrics because they occur before development teams start instrumenting their software development and delivery processes.

Administrative Process Challenges

In addition to funding, some DoD software factories cited significant delays caused by processes for establishing agreements with platform users. For example, some Air Force interviewees regarded the federal interagency agreement process (based on FS Form 7600A) as introducing too much overhead, since it needs to go to the major commands (MAJCOM) for approval and can consequently take up to six months. They felt it was better to use the interagency quote from the pipeline development team as the agreement, which can be signed at the GS-14/15 and O-5 level and processed in 30 days.

DoD also generally contracts for vendors to develop software using either vendor-provided or government-provided operating services. However, changes required for National Institute of Standards and Technology (NIST) SP 800-218, “Secure Software Development Framework,” and for Executive Order 14028, “Executive Order on Improving the Nation’s Cybersecurity,” may result in DoD providing software development capabilities, services, or tools to vendors through DoD Components or organizations. These issuances have not yet been widely established or validated, which creates an excellent early opportunity to instrument their use to understand the executability of the associated business processes and the overall effectiveness of these approaches. The goal is for the government to own the means of production while contractors and the DIB provide domain expertise using DoD software factories and DevSecOps platforms.

The Need for Transparency

Clear and consistent shared expectations between all parties is key to the success of DoD software factories and platform customers alike. Several participants in our study wanted to see increased transparency regarding the capabilities and limitations of existing CI/CD pipelines to enable the customers to make better-informed choices. This call for transparency has been a common refrain in prior engagements.

Customers would also like to see some mechanisms in place to address non-performance. In a contractor-operated environment, it's possible to incentivize behavior. This isn't possible in inter-government relationships. For example, unfortunate situations have occurred where issues such as understaffing (as noted in the prior section) resulted in significant delays affecting the ability of the software factory to execute on their mission in a timely fashion consequently affecting the customer.

The desire for increased transparency applies not only to clearly documenting technical tradeoffs and limitations but also to the success of services provided to other programs. One suggestion was that Quality Assurance Surveillance Plans (QASP) and Contractor Performance Assessment Reporting Systems (CPARs) could be applied to internal service providers in addition to contractors.

4.6 Improving Financial Transparency

The variety of mechanisms organizations have used to purchase cloud services presents a challenge to obtaining utilization data. This challenge makes it difficult to report and model costs, which in turn affects capacity planning. Mismatches between planned and available capacity can result in either unnecessary spending or failure to deliver capability. There are several initiatives underway to improve collection and reporting of utilization data and thereby, provide the transparency and accuracy necessary to effectively align mission needs, staffing requirements, and IT investments. These initiatives include the following:

Cloud FinOps: DoD is in the process of launching a strategic Cloud FinOps Initiative.[20] This effort will focus on improving and standardizing the collection and reporting of utilization data; defining metrics, targets, and models; sharing data; and integrating insights for effective governance.

Digital Innovation Adoption Kit: The Navy PEO Digital Innovation Adoption Kit includes many useful concepts for IT enterprise management that can potentially transfer to other enterprise efforts. The Kit offers guidance for assessing IT investments to inform strategic investment decisions, resource allocation, and system decommissioning. World-Class Alignment Metrics (WAMs)[21] collect data from mission outcomes.

4.7 Baseline and Moving Forward

Software factories today employ widely different funding models that are often combined in novel ways, making it difficult to measure or quantify the "best fit" approaches for delivering value in different contexts. Inconsistent mechanisms for reporting utilization of cloud-based services contribute to the complexity. We have some insight into the efficacy and fitness of these different approaches in different contexts but need to continue gathering data.

Optimizing the DoD software factory ecosystem requires the ability to make informed decisions to support the alignment of software factory assets with mission needs and maintain the ability to adapt to changing conditions. This ability requires gathering data on the funding/business models in use and their relationship to real mission outcomes. Collecting consistent data on utilization, staffing, execution, and outcomes should allow for meaningful analysis of existing capacity at

[20] The FinOps Foundation describes FinOps as "an operational framework and cultural practice which maximizes the business value of cloud, enables timely data-driven decision making, and creates financial accountability through collaboration between engineering, finance, and business teams." As defined in the FinOps Foundation's FAQ, "FinOps is a portmanteau of 'Finance' and 'DevOps,' stressing the communications and collaboration between business and engineering teams.... Other names for the practice include 'Cloud Financial Management,' 'Cloud Financial Engineering,' 'Cloud Cost Management,' 'Cloud Optimization,' or 'Cloud Financial Optimization.'" https://www.finops.org/introduction/what-is-finops/

[21] Use of WAMs provides several advantages. First, WAMs offer a standard measuring methodology that also links technology outcomes to the mission outcomes they produce. Second, low-level data that has operational value can, when aggregated, support portfolio management. Third, WAMs metrics have been associated with data sources, both manual and automated (e.g. ticketing systems).

individual organizations and across the DoD software factory ecosystem. This should help DoD better understand the efficacy of various funding models and support data-driven governance decisions that ensure support and resources sufficient to meet mission needs now and in the future. Scaling proven practices will speed the growth and adoption of DevSecOps with common funding and acquisition models, common workforce management, and streamlined access to portfolio offerings. It's imperative for the entire Department—through the cooperation of all DoD Components—to implement and execute complementary policies, guidance, and practices in this area (as noted in section 4.4).

The DoD software ecosystem and portfolio data collection efforts underway across the DoD Components, along with ongoing efforts to improve the collecting and reporting of utilization and cost data (e.g., the FinOps Strategy and the Navy PEO Digital's Innovation Adoption Kit), create an opportunity to collaboratively develop these insights. In the interim, it may be helpful to investigate the business/cost models of some modern software organizations in the DoD and other federal organizations. DoD may be able to leverage novel methods used by these organizations for estimating workload, staffing, and workforce needs. When innovative cost and business models are used, it is critical to instrument them against desired outcomes to evaluate effectiveness.

Comprehensive efforts are well underway across the DoD Components to collect and characterize enterprise inventories of their software factories to enable strategic governance. These efforts have included time-intensive, manual data collection activities involving meetings, surveys, and listening tours, but they are necessary to develop a comprehensive landscape and establish initial baselines. Achieving a comprehensive enterprise inventory of the DoD's software factories and DevSecOps platforms—and leveraging automation and federated data feeds to help keep it updated—is entirely possible through the combined efforts of the DoD Components. The development of a baseline set of common, goal-oriented "reference metrics" could further facilitate such analysis.

Collecting quantitative status data and qualitative feedback in the following four areas can further accelerate the delivery of mission capability by uncovering and sharing proven, evidence-based practices to reproduce and scale successful patterns across DoD:

Program and Project Management: Approaches for allocating and monitoring resources across projects; risk management; customer-facing "product management" activities for understanding and prioritizing requirements; and DevSecOps "product ownership" activities for ensuring predictable deliveries of quality products and services.

Architecture and Technology Management: Practices for DevSecOps technical architecture, cybersecurity engineering, and compliance.

IT Operations: Insights on lessons learned and successful innovations for operations and management of DevSecOps engineering pipelines and operational environments.

Investment Management: How DevSecOps is considered in the broader mission requirements planning and investment processes (e.g., as managed by a "CIO Council" or other strategic enterprise forums). We want to understand how software factories are tying the value of their DevSecOps activities to defense missions.

Section 8 presents a more extensive discussion of data collection and measurement needs.

5 DevSecOps Enables a Cybersecurity Transformation from Point-in-Time Risk Assessment to Continuous Authority to Operate

5.1 The Importance of cATO

Authorization to Operate (ATO) manages risk by assuring that a system in an environment complies with Federal Information Security Management Act (FISMA) requirements. ATO provides a level of transparency enabling the mission owner to evaluate the tradeoffs of risk versus the cost of not using the system. Current ATOs largely focus on obtaining system authorization at a point in time, but they don't address the continuous management of system cybersecurity risk established by the NIST Risk Management Framework (RMF).

The cATO memorandum from February 2022 specifically addresses the three competencies needed for continuous authorization, which is critical to "achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces." cATO is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in its ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust, continuous information security monitoring capabilities; active cyber defense; and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system's cyber posture.

The DoD CIO has worked with community partners on the evaluation of cATO environments and has developed evaluation criteria along with use cases and guidelines for evaluating a request for continuous authorization for organizations using DevSecOps. In addition to the "cATO Evaluation Criteria" publication, the DoD CIO has published a cATO Implementation Guide for implementers of systems that seek a cATO. It provides an overview of cATO key practices and assessment procedures.[22]

DoD Components are actively applying the new cATO evaluation criteria to their software activities. Several programs have been submitted as pathfinders.

5.2 The cATO Process

The cATO process is meant for systems built by programs or software factories that practice DevSecOps, and it can apply to all software domains, including weapons systems and business systems. To obtain a cATO, the system must have an existing ATO and have entered the RMF monitoring stage. There are three main competencies that must be demonstrated by the Authorizing Official: ongoing visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in real time; and the adoption and use of an approved DevSecOps reference design.

Continuous Authority to Operate is a significant shift in DoD cybersecurity practices.

It requires a tremendous amount of coordination across organizational boundaries with diverse goals, cultures and policy interpretations.

Transformational leadership is a key success factor for CaTO.

Successful examples of achieving ATO include strong leadership highlighting shared objectives, clear understanding of the objectives, and frequent collaboration across boundaries.

DoD leaders have their ear to the ground:

The DoD has heard the challenges raised by the community and is working to address them through policy, guidance, pathfinders, and establishment of metrics to assess cATO effectiveness.

[22] Evolving guidance and related resources on cATO will be published on the RMF Knowledge Service (KS) at https://rmfks.osd.mil as well as in the DoD CIO Library.

5.3 The cATO Assessment Method

These competencies must be demonstrated through a cATO assessment, which requires the formation of an assessment team comprising a multidisciplinary group of members with the appropriate knowledge and skills to assess the DevSecOps platform, processes, and people. This team should be trained on the cATO process and familiar with analysis of the cATO evaluation criteria. The team must also submit an assessment plan. A high-level summary of the evaluation criteria for cATO requires that practices are defined and documented; evidence exists on the use of risk management and continuous monitoring practices, with demonstrations; the workforce is knowledgeable on the cATO practices; and the level of implementation of the cATO risk management practices has been reviewed for effectiveness. The assessment must be coordinated with the responsible cATO office, and the assessment plan must be reviewed for completeness. Additional details of the cATO assessment method can be found in the "cATO Implementation Guide." Figure 5-1 summarizes the cATO assessment method.

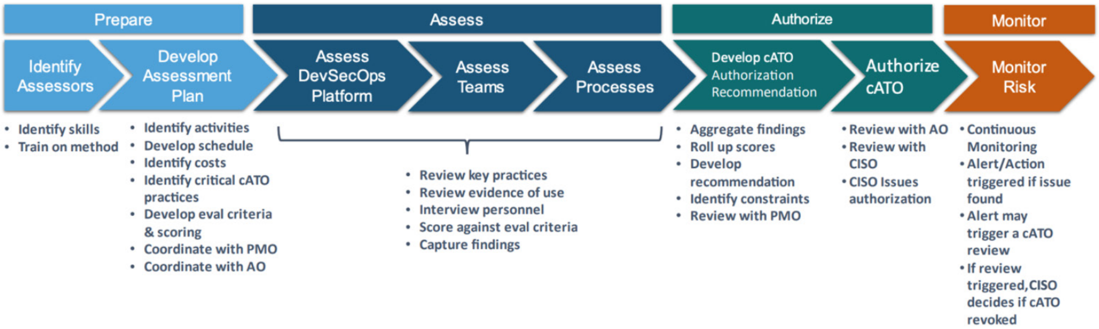


FIGURE 5-1: CATO ASSESSMENT METHOD

5.4 Barriers and Challenges to cATO

The barriers and challenges to cATO commonly discussed by the community are understandable considering the planning, collaboration, and strong leadership necessary across all stakeholders to execute a cATO evaluation. DevSecOps isn't only a key competency of cATO, it also requires a socio-technical culture that provides the framework cATO depends on. All the activities described in the cATO assessment method can't happen in a vacuum or silo. It takes a tremendous amount of coordination across every stakeholder in a DevSecOps organization. Too often, cybersecurity teams, IT infrastructure teams, development teams, leadership, AOs, and DoD Component CISOs don't engage in a collaborative manner, which is necessary to achieve cATO. The cATO competencies are tightly coupled with continuous DevSecOps activities, which requires shared responsibility, accountability, execution, monitoring, and evaluation.

Additional challenges regarding cybersecurity risk management stem from mismatch/misalignment in culture and interpretation: cybersecurity specialists and software developers have different responsibilities and expertise and so place different emphasis on trade-offs. For example, it is a common refrain that AOs are "biased to caution" rather than "biased to action" resulting in delays of software capabilities. It's not that the developers want to release products that will be vulnerable, but that their primary consideration is speed of meeting the mission need through the creation, delivery, and deployment of software.

The primary objectives of IT Operations include stability, accessibility, and availability of infrastructure used by all stakeholders. The commanding officer has ultimate approval but will frequently defer to the AO unless there is an emergency.

Success Story: Driving towards continuous Authorization of Weapons Systems

Naval Sea Systems Command (NAVSEA) assessed and approved multiple software factories in CY24 following DevSecOps standards. Using the Afloat Software Authorization Playbook (ASAP) process, NAVSEA software factories are rapidly delivering new software solutions for afloat and ashore programs, supporting the acquisition and operational needs of the Navy's surface and submarine fleet.

This streamlined process has significantly reduced the time required to deploy critical software updates, enhancing the fleet's operational readiness and capability. The forward leaning programs that have adopted the DevSecOps standards have demonstrated improved software quality and security, ensuring that the Navy's systems remain resilient against emerging threats. A NAVSEA team delivered 13 updates to an application in one of NAVSEA's production clouds over the last 9 months. They are also rapidly iterating software in Research Development Test & Evaluation (RDT&E) with features/bug fixes developed and delivered in 24-48 hours, farm-to-table.

5.5 Reciprocity Challenges

Reciprocity is defined as the "agreement among participating organizations to accept each other's security assessments, to reuse system resources, and/or to accept each other's assessed security posture to share information."[23] Many people we interviewed, and attendees at the June 2024 Software Factory Coalition Summit, openly discussed challenges and successes associated with meeting reciprocity goals. Common discussion points included lack of reciprocity and cases in which reciprocity guidance was unclear, leading to uncertainty with how assessors and AOs would interpret guidance (e.g., when controls could be inherited). The lack of reciprocity between the Military Services prevents mission owners from making their own decisions, and it blocks developers from using tools developed at other Military Services. An interviewee described an instance of cross-Military Service ATO authorization taking several months—common frustration.

The reciprocity problems noted across the DoD community have been heard. In the May 2, 2024, memo, "Resolving Risk Management and Cybersecurity Reciprocity Issues," the Deputy Secretary of Defense directed that reciprocity be the default stance, "except when cybersecurity risk is too great," and further directed that when reciprocity issues can't be resolved by the DoD Component-level CIOs, they be elevated directly to the DoD CIO for resolution. The Cybersecurity Reciprocity Playbook assembles reciprocity use cases, guidance on AO roles and security configurations, and information resources to facilitate reciprocity activities—as well as providing a feedback mechanism for community members to share innovative ideas and opportunities for enhancement. Additionally, the Army has established policy to recognize ATO reciprocity across the Army. We are hopeful this guidance will accelerate adoption by the DoD community so it can begin to realize the benefits of leveraging reciprocity.

5.6 Baseline and Moving Forward

Prior to the 2022 cATO memo, several DoD software factories were operating in a fashion aligned with cATO but inconsistent across DoD Components. The memo clarified expectations from the DoD CISO, building on practices reviewed by DoD Component CISOs focused on how software factories managed changes across their people, processes, and practices. Those programs are still operating their continuous ATO as the updated cATO is adopted, and they are demonstrating enhanced security and identifying attacks to the DoD software supply chain faster than traditional programs.

With the release of updated criteria, DoD is waiting for DoD Component CISOs to nominate software factories demonstrating the appropriate continuous monitoring, active cyber, and DevSecOps practices. These nominees will become the pathfinders that other programs can model and learn from. Those pathfinders will continue to evolve and mature cATO processes, increasing their security and speed of delivery. The Office of the DoD CIO has reviewed several candidates and is enthusiastic about their potential to significantly improve the quality of DoD software and protection of DoD assets.

Pathfinder cATO software factory measures will include lead times and process flow status to help software teams plan and negotiate commitments. At the enterprise level, this data will provide

[23] Department of Defense. "Cybersecurity Reciprocity Playbook." Department of Defense. May 15, 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf

visibility into improvements in the timeliness of cATO approvals, which will help enable further performance improvement opportunities.

Organizations don't have to provide metrics for cATO effectiveness, but we are interested in potential metrics to evaluate the effectiveness of the cATO process from a DoD governance perspective. These metrics include the following:

- Cyber hygiene metrics, such as Mean Time to Patch Vulnerabilities, measure the average time between the identification of a vulnerability in the software product and the successful production deployment of a patch. These metrics focus on vulnerabilities with high to moderate impact on application or mission.
- Trend metrics associated with guardrail and control gate results over time show improvements in development team efforts to develop secure code with each new sprint and the system's continuous improvement in its security posture.
- Feedback communication frequency metrics ensure feedback loops are in place, being used, and trends toward improvement in security posture.
- Mitigation metrics measure continued effectiveness of mitigations against a changing threat landscape.
- Security posture dashboard metrics show status of application and its security posture in the context of risk tolerances, security control compliance, and security control effectiveness results.

Outcome measures include counts, severity, and types of security for all systems and for systems with cATO. Much of the relevant operational data should be available in existing issue tracking systems.

6 Policy and Guidance Enables Change

DevSecOps adoption requires DoD to take a holistic approach to enabling change that encompasses tools and technologies, culture, skillsets, processes, funding mechanisms, and inter-organizational dynamics. Policy and guidance are central to enabling change, including change in the acquisition of technical assets and in the recruitment, training, and retention of staff experienced in modern software practices.

A key theme we identified with study participants was the need to approach policy and guidance in a manner that aligns with the nature of DevSecOps and addresses the challenges of DoD adoption. Participants emphasized the need for policy and guidance to accommodate feedback loops and bottom-up input. They also emphasized the need for policy and guidance to account for the array of technical challenges across the DoD portfolio and the different levels of technical and cultural adoption readiness. This section summarizes participants' thoughts on how best to create and implement effective DoD DevSecOps policy and guidance.

DoD is harvesting grassroots successes to develop broadly applicable policy and guidance.

The Software Factory Coalition working group and the DoD DevSecOps Community of Practice are forums where bottom-up innovation enables and informs top-down change.

6.1 Scaling Grass Roots Innovation

The collaborative and innovative spirit across DoD DevSecOps community leadership has been a driving force in establishing the software factory ecosystem, in bringing forth creative solutions to common challenges, and in enabling and encouraging open dialog as a broad community of practice. The Software Factory Coalition is a grass-roots collaborative organization in which DoD software factories and DevSecOps platform teams can share experiences, problems, and potential solutions. Participants gather together from across DoD DevSecOps organizations. It also includes participants from academia and FFRDCs. Key DoD leaders are engaged and accessible to listen to challenges, collect feedback, and gather experiences on success stories, all of which contribute to the development of policy and guidance efforts to accelerate DevSecOps adoption and benefits. In the DoD-sponsored DevSecOps Community of Practice, participants gather for monthly virtual meetings to share updates on strategies and initiatives that affect the DevSecOps community and hear from practitioners. These meet-ups regularly host hundreds of participants. The regular communication mechanisms foster connections and community spirit among the DevSecOps community and DoD leadership, enable rapid feedback loops between leadership and teams, encourage sharing of ideas across the community, and are an important mechanism for disseminating information about policy and intent.

Culture interprets policy.

When working across organizational boundaries, it's important to develop shared visions of success that take into account goals, incentives, and operational needs of all stakeholders.

We can change culture.

Understanding cultural context for different stakeholders enables us to deliberately design the culture change we need.

6.2 Policy at the Speed of Relevance

As members of the community responsible for understanding and implementing policy, study participants addressed the challenges they face interpreting policy and the role bias and expertise (or lack of it) play in their ability to effectively apply policy and guidance. They spoke of the distinctions between intent-level, aspirational guidance, and the need for guidance that reflects current operational realities. They also discussed the need for policy and guidance to keep pace with the rapidly changing technology and threat environment.

From these conversations, 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.

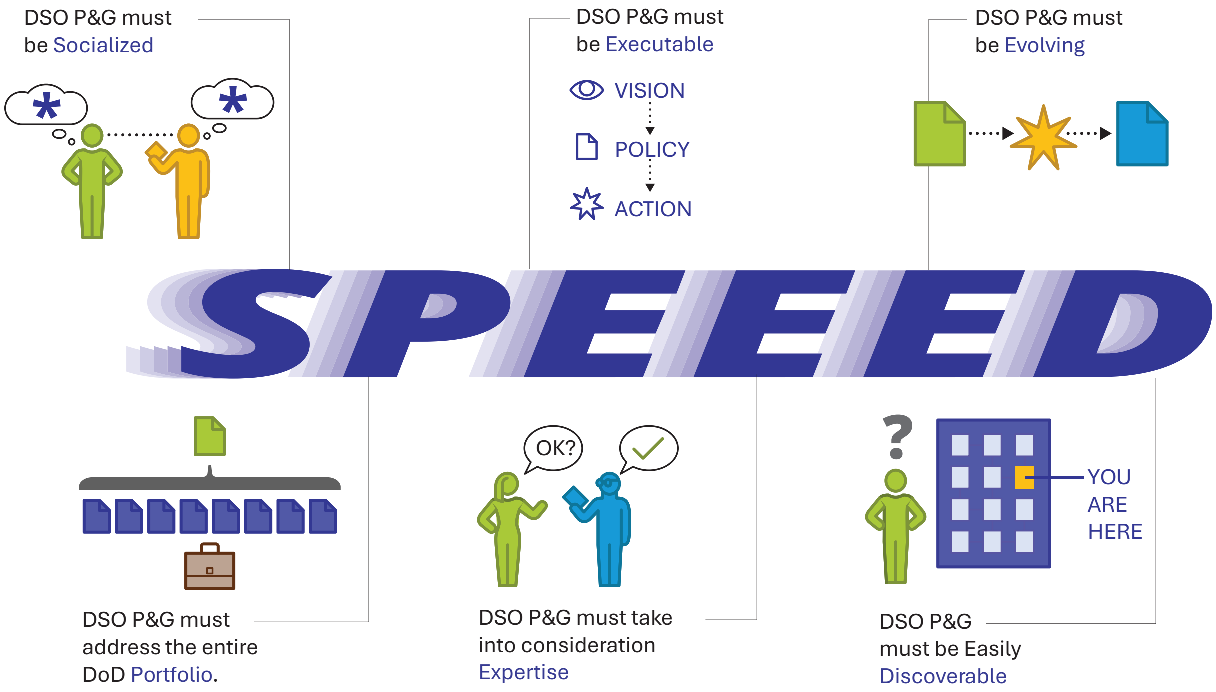

DSO P&G must be Socialized
DSO P&G must be Executable
VISION
POLICY
ACTION
DSO P&G must be Evolving
SPEEED
DSO P&G must address the entire DoD Portfolio.
OK?
DSO P&G must take into consideration Expertise
YOU ARE HERE
DSO P&G must be Easily Discoverable

FIGURE 6-1: THE NEED FOR SPEED

The Need for S-P-E-E-E-D

1. DevSecOps policy and guidance must be Socialized.

While participants generally applauded DoD's DevSecOps strategic-level "intent" issuances, they expressed concern that cultural preconceptions and filters may prevent this intent from being reflected in lower-level "execution" issuances. They expressed the need to make sure that policy is fully understood across organizational levels and functions—both the letter of the policy and the underlying cultural underpinnings.

2. DevSecOps policy and guidance must address the entire DoD Portfolio.

DevSecOps policy and guidance must address the broad range of DoD systems and the impact of that on CI/CD pipeline technologies and software development life cycles. Where policy is specific to certain types of applications and systems, the context of applicability should be clearly spelled out.

3. DevSecOps policy and guidance must be Executable.

While strategic-level policy and guidance may be visionary in nature, operational-level policy issuances should be executable based on current capabilities and limitations. Policy that can't be implemented will be ignored or will generate frustration.

4. DevSecOps policy and guidance must take into consideration implementor Expertise.

Policy and guidance are ultimately used to support decision-making. However, the technical and domain expertise of decision makers often impacts policy interpretation. Without the technical knowledge to assess the impact of various options, decision makers may tend to play it safe, avoiding risks they're not fully equipped to weigh. Highly prescriptive IF-THEN-ELSE type guidance isn't a viable approach to complex DevSecOps environments and challenges. Appropriate training and expertise is critical for effective interpretation and execution of policy and guidance issuances.

5. DevSecOps policy and guidance must Evolve.

Policy and guidance must be able to rapidly evolve in response to internal DoD feedback, changing technology, and changing mission imperatives. Establishing goal-oriented measurement and feedback mechanisms is critical to enabling this flexibility.

6. DevSecOps policy and guidance must be easily Discoverable.

Access to DevSecOps policy and guidance should be straightforward with easy-to-use search and navigation tools, and update notification mechanisms. Policy and guidance must not only evolve at the pace of DevSecOps technology and environmental challenges, it must also be consumed and enacted at the same pace.

6.3 Culture Interprets Policy

An understanding of an organization's underlying culture is critical to enabling change as well as to issuing policy and guidance. Before policy can be executed, it must be disseminated and interpreted, and culture is a major influence on this interpretation. Successful execution of DevSecOps relies on collaboration and shared responsibility across all aspects of the pipeline. As one of our participants put it, "Culture interprets policy." In the course of our work, cultural interpretation was seen as impacting two major areas: translating policy and guidance vision into execution and achieving collaboration.

FIGURE 6-2: CULTURE INTERPRETS POLICY

Translating Strategic Intent and Vision into Executable Policy and Guidance

Several participants in the study indicated that culture may block the implementation of strategic vision created by leadership through the creation of lower-level policies that don't align with the high-level intent. They indicated that "execution-level" policy, was often written from a more control-oriented, hardware-focused, and waterfall-based perspective, distorting the original vision:

> *"The intent is good news. The intent is changing the narrative, but that intent that has not trickled down to the tactical implementation level. You may have a policy at the DoD level that is very broad, but there can be a lot of constraints added between the DoD level and the implementors."*

The MEPCOM success story in Section 2, exemplified these added constraints in the initial execution of the hiring process, in which many of the subject matter experts were unfamiliar or uncomfortable with using new staffing practices.

Achieving Collaboration Across the DevSecOps Enterprise

Cultural disconnects between organizations can significantly impact pipeline effectiveness and flow. Study participants frequently cited such disconnects between development organizations and functions such as cyber, test and evaluation, finance, and acquisition, and residual legacy statute, policy, and practice. The following represent a small sample of quotes from study participants:

> *" I am agile up to the point of being tested. I go super-fast up till test and compliance."*
>
> *"AOs ...[are]... removed from the consequences of not having a given app—so their only incentive is to achieve security or not approve it at all."*
>
> *"[We are] told to take risks and upset the apple carts... but contradicted by the ITAS (Information Technology Approval System) not trusting us to make a decision over $500.00."*

These examples illustrate a tension between goals and incentives associated with accelerating the speed of delivery/execution versus goals and incentives associated with minimizing risk. Understanding the sources of these disconnects is the first step in enhancing collaboration across organizational boundaries.

In the next section, we provide a brief introduction to an established model that can help leaders and teams reduce conflicts and improve collaboration through a better understanding of organizational culture.

6.4 Understanding and Aligning Culture

The Competing Values Framework (CVF) is a model we can use for understanding, and ultimately aligning, organizational cultures.[24] The underlying thesis of the CVF is that organizational culture is based largely on the concept of value and informs the answers to the following questions:

[24] Cameron, K. S.; Quinn, R. E.; Degraff, J.; & Thakor, A. V. "Competing Values Leadership" (3rd ed.). Edward Elgar Publishing. 2022. https://search.worldcat.org/title/1328022320

- What value does my organization deliver?
- What skills and activities deliver value?
- What behaviors and interactions are valued?
- How do I become valued in my organization?

The CVF is a quadrant organized along two axes, as shown in Figure 6-3. The vertical axis represents an organization's orientation relative to Individuality and Flexibility versus Stability and Control. The horizontal axis represents whether the organization is primarily internally or externally focused.

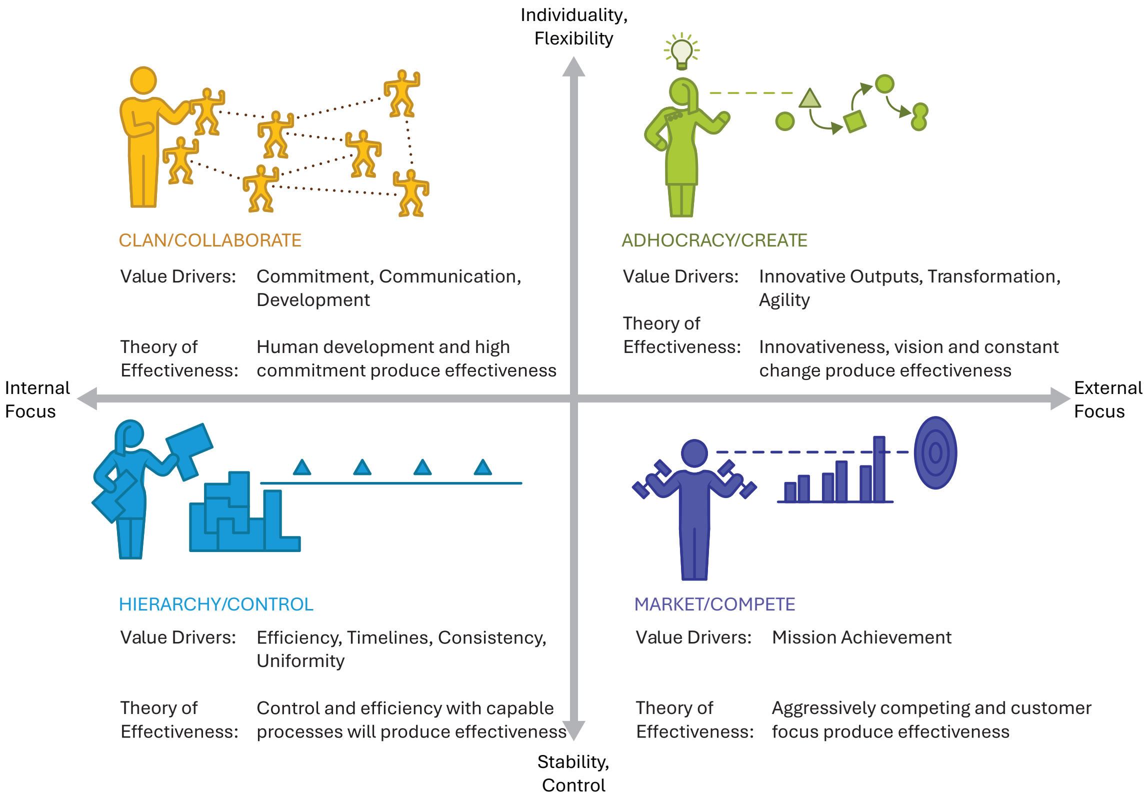

Individuality, Flexibility
CLAN/COLLABORATE
Value Drivers: Commitment, Communication, Development
Theory of Effectiveness: Human development and high commitment produce effectiveness
ADHOCRACY/CREATE
Value Drivers: Innovative Outputs, Transformation, Agility
Theory of Effectiveness: Innovativeness, vision and constant change produce effectiveness
Internal Focus
External Focus
HIERARCHY/CONTROL
Value Drivers: Efficiency, Timelines, Consistency, Uniformity
Theory of Effectiveness: Control and efficiency with capable processes will produce effectiveness
MARKET/COMPETE
Value Drivers: Mission Achievement
Theory of Effectiveness: Aggressively competing and customer focus produce effectiveness
Stability, Control

FIGURE 6-3: COMPETING VALUES FRAMEWORK

The quadrants that result from mapping the two axes are as follows:

- The Clan/Collaborate Quadrant is Internally focused with an emphasis on Individuality and Flexibility. This Quadrant's Value Drivers are Commitment, Communication, and Personal and Organizational Development.
- The Hierarchy/Control Quadrant is Internally focused with an emphasis on Stability and Control. This Quadrant's Value Drivers are Efficiency, Timelines, Consistency, and Uniformity.
- The Adhocracy/Create Quadrant is Externally focused with an emphasis on Individuality and Flexibility. This Quadrant's Value Drivers are Innovative Output, Transformation, and Agility.
- The Market/Compete Quadrant is Externally focused with an emphasis on Stability and Control. This Quadrant's Value Drivers are Mission Achievement.

The transition from waterfall to agile development and then DevSecOps can be viewed as transitioning from a culture dominated by Control-oriented values (DoD's traditional hierarchical control culture) to one that incorporates the values of the Creative and Competitive quadrants.

Up above, we discussed organizational conflicts that impact flow across the DevSecOps process. Under the CVF this can be understood as disconnects between the Creative/Competitive stance of Development and Mission-focused organizations, and the Control-oriented stance of organizations responsible for test and evaluation, cyber, compliance, certification, finance, etc. While mission-focused participants understood the requirement for oversight and risk control, they stressed the need to balance control and risk reduction with innovation, speedy execution, and reduced time to delivery.

Similarly, culture comes into play in the disconnects cited between strategic issuances reflecting Creative/Competitive perspectives and the Control-oriented cultures of the implementing organizations.

6.5 Integrating Cultures to Achieve Transformational Value

Leadership plays a critical role in integrating cultures and organizations. Through this integration, enterprises are able to achieve outcomes that transcend what can be attained by focusing on the skillsets of a single quadrant.

In particular, the CVF states that leaders must demonstrate:

- **Transformational Thinking:** The ability to move from “either / or” to “both / and” thinking.
- **Empathy and Influence:** The ability to help others recognize and identify new opportunities for value that transcend the culture of their quadrants.

While participants shared many similar stories of conflicts between organizational culture and priorities, they also shared stories demonstrating the leadership skills and transformational thinking required to achieve alignment. The two success stories in the green boxes to the right describe collaboration across organizational boundaries to devise solutions that aligned the values of all organizations; specifically, the goal of the software organization to move at speed with the need to provide the cybersecurity, test, and certification organizations the information necessary to make informed assessments about risk.

In addition to participants’ stories, there is the pilot effort underway in which DOT&E and the DoD API Tiger Team are collaborating to develop a software testing metrics infrastructure to enable faster, easier performance analysis through Developmental and Operational Testing (DT/OT) without requiring experience with unfamiliar DevSecOps tools. This pilot program is marrying the goals of accelerating software delivery via DevSecOps with the goals of the testing organizations by making necessary data available at an accelerated pace.

6.6 Baseline and Moving Forward

As illustrated throughout this document, DoD has undertaken a number of DevSecOps-related change efforts and initiatives. These efforts could be further advanced and supported by working to understand how culture can obstruct or accelerate change and how policy and guidance can be couched in a change management context.

> You need to build a culture that gets Operational Test, Pen Testers, and certifiers involved. I brought cyber into sprint reviews and the Authorizing Official was there as well. I tried to have cyber folks understand they are agile too.
>
> *— Anonymous*

> The RMF process was going to be the bottleneck. We looked at the NIST 853 controls and identified 100 controls that were required at the application layer. We baked those into our pipeline for automated control and testing. Then we continuously monitor and make sure the controls stay up to date.
>
> *— Anonymous*

7 Forging a Mission-Ready DevSecOps Workforce

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. A skilled, motivated, and well-supported workforce is essential for implementing and sustaining DevSecOps practices across the DoD. As we navigate an increasingly complex threat landscape, the ability to recruit, retain, and continuously develop top-tier talent becomes critical to our mission success.

The Defense Innovation Board's SWAP study highlighted the unique challenges faced by software professionals in the DoD, emphasizing the need for specialized career paths and continuous support. In response, DoD has initiated several strategic efforts to build a robust DevSecOps workforce, focusing on recruitment, retention, and professional development. This section provides an overview of the current state of the DevSecOps workforce, recent accomplishments, and ongoing challenges.

7.1 Current State of the DevSecOps Workforce: Empirical Evidence

To understand the current state of our DevSecOps workforce and establish a baseline, we conducted interviews with approximately 30 individuals at 19 DoD software factories and software organizations. The results mirror the concerns raised in the SWAP study, which provided compelling evidence motivating the significant efforts of the DoD to modernize the recruitment, hiring, and career paths of software professionals. We also discovered that the concerns articulated by study participants were recognized by the DoD, and changes to modernize workforce management are underway. We will first summarize the baseline findings then summarize the modernization efforts.

Recruitment and Hiring

Managers report that recruitment and hiring have been hampered by a recruitment process that was not focused on identifying specialty software skills, a long hiring process, and delays in onboarding. Recruitment had been modernizing organically. We found successful leaders who were effective not only in identifying alternate sources for software talent but also in working with DoD hiring professionals to use these alternate sources and accelerate the hiring process.

This ability was characterized as "finding a way to say, 'yes'" while advocating for new approaches. This highlights the crucial need for non-technical business skills among leaders, which suggests one reason technical managers may struggle with software modernization efforts. The recruitment and hiring process especially has been challenging. The participants expressed concern that the legacy recruiting processes did not support the non-traditional venues at which software talent could be found. They also noted that the extended hiring process within the DoD was not designed to accommodate the pace of hiring a high-demand software professional. When asked about the biggest risks their organizations face, 20 percent of the participants pointed to the long hiring lead time, which can result in potential candidates accepting opportunities elsewhere.

Retention

Participants cited retention as another common concern. In our interviews, 68

DoD is enacting strategic workforce initiatives.

The DoD has made significant strides in building a robust DevSecOps workforce, driven by the DoD Cyber Workforce Strategy Implementation Plan. Key initiatives include new software work roles, targeted recruitment strategies, and enhanced retention programs.

Supportive workforce development is a top priority.

Continuous learning and professional development are prioritized through training programs, on-the-job experience, and mentorship. Initiatives like the Army and Marine Corps Software Factories are demonstrating innovative approaches to growing the Department's DSO workforce.

percent of the participants cited pay disparity with similar positions in industry as a reason for staff leaving. For example, one team leader claimed that only 40 percent of the military staff chose to reenlist after their tour, opting instead to pursue a higher salary in the commercial sector. The ability to quantify the issue became one of the goals in the modernization effort.

Interviewees consistently stated that the lack of defined career paths within the DoD for technical roles was another key factor impacting retention. Personnel, particularly civilians, expressed concerns about reaching a plateau in their careers. Military personnel faced other barriers, including assignment rotations and advancement opportunities misaligned with enlistment timelines. Lack of career progression not only results in the loss of skilled technical professionals but creates knowledge gaps, including a lack of senior leaders.

Workforce Development

Accessible and relevant training is key to developing workforce talent. While the DoD offers training programs like Digital University and the Defense Acquisition University (DAU), interviewees emphasized the need for training that is readily accessible, immediately applicable, and of high quality.

Practical experience gained through on-the-job training (OJT) and mentorship was considered invaluable for developing proficiency in DevSecOps. However, providing adequate mentoring proved challenging due to the high workload placed on senior technical staff. Interviewees cited contractual constraints that sometimes limits government and contractor collaboration in mentorship roles.

At the time of this report, the DoD is aware of the challenges, and workforce modernization is well underway. The next section briefly describes these efforts.

7.2 Strategic Workforce Modernization Initiatives

In 2023, the DoD CIO released the DoD Cyber Workforce (CWF) Strategy and associated Implementation Plan. These documents form a comprehensive blueprint for developing and sustaining a skilled cyber workforce as defined in DoDD 8140.1. (Figure 7-1, on the next page, illustrates the comprehensive elements of the strategy.) The CWF Implementation Plan include objectives, initiatives, and key performance indicators (KPIs) aimed at baselining and improving identification, recruitment, retention, and professional development in accordance with the workforce qualifications defined in DoDM 8140.03. Notable advancements include the introduction of new software work roles under the DoD Cyber Workforce Framework (DCWF), which enhances the tracking of expertise and facilitates more focused recruitment and training strategies.[25]

> To recruit and retain the most talented workforce, we must advance our institutional culture and reform the way we do business. The Department must attract, train and promote a workforce with the skills and abilities to tackle national security challenges, creatively and capably, in a complex global environment.
>
> *— Mr. Lloyd Austin, III*
> *Secretary of Defense*

Recruitment and Hiring

Efforts to recruit talent for DoD software factories and other DevSecOps roles have become more creative and targeted. The introduction of new roles, such as DevSecOps Specialist and Software/Cloud Architect, has enabled better tracking of expertise and facilitated more focused recruitment strategies. Hiring timelines remain a challenge, with the average duration to extend job offers still exceeding desired targets. The CWF Implementation Plan sets a goal to reduce time-to-hire to 60 days by FY27, reflecting the ongoing need to streamline and expedite the hiring process. Innovative programs such as the Public-Private Talent Exchange are being used across the Department to bring in short-term expertise from industry and to grow DoD talent through immersive cohort assignments.[26]

[25] Austin sidebar quote: Department of Defense. “DoD Cyber Workforce Strategy.” Department of Defense, CIO. March 1, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

[26] Office of the Under Secretary of Defense. “Public-Private Talent Experience.” OUSD Human Capital Initiatives website. October 3, 2024 [accessed]. https://www.hci.mil/ppte.html

Retention Strategies

Retention remains a top priority, particularly given the competitive landscape for technical talent. The mission itself is a powerful motivator, and many developers cite their commitment to national defense as a key reason for staying. Salary disparities between government and industry, along with career path limitations, present ongoing challenges. The CWS Implementation Plan addresses these issues by enhancing financial incentives, promoting career development programs, and expanding remote work opportunities to improve retention rates.

Workforce Development

To sustain and grow the DevSecOps workforce, DoD has prioritized continuous learning and professional development. Training programs, such as Digital University and various boot camps, offer flexible, on-demand learning opportunities that align with the qualifications defined in the DoD 8140 policy series.

Additionally, OJT and mentorship play crucial roles in skill development. The Education and Training Software Factories exemplify a successful approach, combining formal training with hands-on experience to prepare the next generation of DoD software engineering professionals.

Success Story: DAU Training Modernization

Defense Acquisition University (DAU) recently updated its major IT and software curricula to make them more accessible across the workforce and to incorporate modern, agile software development practices. This update includes changes that have been incorporated in its Engineering and Technical Management, Production Management, and IT Modeling & Simulation focus areas in response to FY23 NDAA Section 835. Mirroring current industry approaches, DAU established “micro-learning” course modules that are typically 10-15 minutes long. In addition, they have forged partnerships with commercial training providers, such as Skillsoft Percipio, Coursera, and LinkedIn Learning, which have yielded over 100 DevSecOps course offerings, simulations, and virtual labs. Since the multiple sources of training and large number of courses can seem overwhelming to the workforce, DAU even created a tool for curating a playlist.

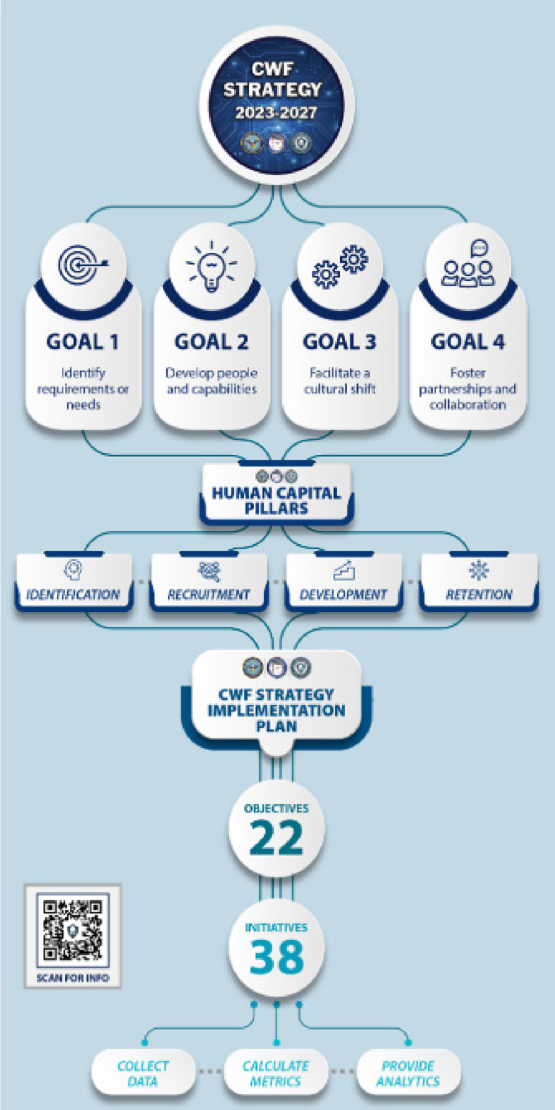


FIGURE 7-1: DOD CYBER WORKFORCE STRATEGY, 2023-2027

7.3 Baseline and Moving Forward

While substantial progress has been made, many improvement actions remain in the early stages of implementation. DoD has established a measurement framework to monitor gaps and track progress, with key indicators including vacancy rates, time-to-hire, turnover rates, and the impact of workforce development programs. These metrics will be critical in assessing the effectiveness of current initiatives and guiding future improvements.

8 A Playbook for Moving Forward

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. This final section is intended to help leaders at all levels effectively collect, transform, and use data to support their organizations and their people throughout our DevSecOps transformation.

To ensure DevSecOps continues to enable mission value, find opportunities to remove barriers to progress, and inform effective decision-making as the mission evolves, we need to explicitly measure against these objectives. Measurement requires data—not just any data, but the right data. Data is a strategic asset that can be used at all organizational levels to aid decision making. What's the right data? It's the data you use every day.

Measures need to connect to value. The Software Acquisition Pathway (and the Army's new software metrics) require the reporting of value metrics in units meaningful to the mission, often as a combination of metrics (not just a single number). We need to take a balanced perspective, encompassing both product outcomes and process metrics, to extract maximum value from available data. Ultimately, the use of data for mission success depends on a combination of rigorous methodology, strategic thinking, appreciation of the domain context, and a deep understanding of the organization's goals and value proposition.

It's tempting to try to aggregate metrics at different levels, but we need to keep in mind that while we can aggregate data to gain different kinds of insights at different levels, the aggregation of metrics may not provide the insight you need. For example, if a business system has a deployment frequency to end users of once per week and a fighter aircraft has a deployment frequency to flight test once per month, taking the "average deployment frequency" between the two isn't meaningful. Understanding the average deployment frequency of like kinds of systems will have value, as will the stability of deployment frequency for individual systems and for like kinds of programs. Aggregating data at higher levels explains where there are differences between contexts—like business systems and fighter planes.

In this section we offer questions that can be used at all levels, from the development teams to acquisition programs to upper leadership, to gain insight into the performance of the DevSecOps ecosystem and identify opportunities to accelerate.

8.1 Getting Insight Into Performance Across the Ecosystem

The table below features questions that can serve as a guide to data gathering and measurement from all parts of the DevSecOps infinity loop. These are just a few examples of information that can be captured to explicitly link DevSecOps organizations with mission outcomes, and should be helpful to leaders in and across stakeholder organizations.

In the next section, we provide a quick reference that leaders can use to think about how to use data to gain insight.

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

TABLE 8-1: DATA LINKING DEVSECOPS ORGANIZATIONS WITH MISSION OUTCOMES

8.2 Using Data Every Day

This guide to using data sums up the key principles we described at the beginning of the section.

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.

8.3 Conclusion

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. In this way, leaders up the chain of command can help scale productive solutions and monitor the system-wide outcomes for success. Mindful, strategic use of data at all levels to understand the health of our DoD software factory and DevSecOps ecosystem will provide the insight we need to prioritize investments, evaluate the effects of policy changes toward their desired outcomes, identify further opportunities to accelerate delivery to the warfighter, and enable rapid adaptation and scaling of innovation to ensure we can rise to meet future challenges.

9 Works Cited and Further Reading

AFCEA. (2024, February 9). U.S. Army officials launch new way to constantly monitor risks. AFCEA Signal Media. https://www.afcea.org/signal-media/cyber-edge/us-army-officials-launch-new-way-constantly-monitor-risks

Bianco, Jessica & Laura Hujber. “Measure and Assess the Effectiveness of Navy and DoD Pilot BA-08 (software) Program Performance.” Naval Postgraduate School website [accessed October 1, 2024]. https://dair.nps.edu/bitstream/123456789/4948/1/SYM-AM-23-176.pdf

Cameron, K. S.; Quinn, R. E.; Degraff, J.; & Thakor, A. V. “Competing Values Leadership” (3rd ed.). Edward Elgar Publishing. 2022. https://search.worldcat.org/title/1328022320

Cowden, Spc. Joshua. “New Data Warfare Company activates as beacon of innovation for XVIII Airborne Corps” (Army Press Release). U.S. Army website. June 9, 2022. https://www.army.mil/article/257441/new_data_warfare_company_activates_as_beacon_of_innovation_for_xviii_airborne_corps

Defense Acquisition University. “Program Management Metrics and Reporting.” DAU website. September 30, 2024 [accessed]. https://aaf.dau.edu/aaf/software/metrics-and-reporting/

Defense Civilian Personnel Advisory Services (DCPAS). DCPAS Homepage. DCPAS website [accessed August 13, 2024]. https://www.dcpas.osd.mil/

Department of Defense. DoD Manual 8140.03 “Cyberspace Workforce Qualification and Management Program.” DoD CIO website. February 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf

Department of Defense. “DoD Cyber Workforce Strategy.” Department of Defense, CIO. March 1, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

Department of Defense. “Software Modernization Implementation Plan Summary.” U.S. Department of Defense. March 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-PlanExecutiveSummary.pdf

Department of Defense. “Cybersecurity Reciprocity Playbook.” Department of Defense. May 15, 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%20 2024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf

Department of Defense. “Structuring Change to Last: An Update on Innovation at the Department of Defense.” U.S. Department of Defense. August 2024. https://media.defense.gov/2024/Aug/07/2003519333/-1/-1/0/DoD-INNOVATION-FACT-SHEET-AUGUST-2024.PDF

Deputy Secretary of Defense. “Resolving Risk Management Framework and Cybersecurity Reciprocity Issues” (memorandum). May 2, 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/ResolvingRMF.pdf

DoD Cyber Exchange. “DoD 8140 Qualification Matrices.” DoD Cyber Exchange (Public) website [accessed August 13, 2024]. https://public.cyber.mil/wid/dod8140/qualifications-matrices/

FinOps Foundation. “What is FinOps?” FinOps Foundation website. October 2, 2024 [accessed]. https://www.finops.org/introduction/what-is-finops/

Forsgren, Nicole; Humble, Jez; & Kim, Gene. “Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations.” IT Revolution. ISBN: 9781942788331. 2018.

Government Accountability Office. “Weapon Systems Annual Assessment: DoD Is Not Yet Well-Positioned to Field Systems with Speed.” GAO-24-106831. Government Accountability Office. June 17, 2024. https://www.gao.gov/products/gao-24-106831

Keller, K.M.; Lytell, M.C.; & Bharadwaj, S. “Personnel Needs for Department of the Air Force Digital Talent: A Case Study of Software Factories.” RAND website. March 30, 2022. https://www.rand.org/pubs/research_reports/RRA550-1.html

Kopp, Carol M. “Seed Capital: What It Is, How It Works, Example.” Investopedia website. August 12, 2024. https://www.investopedia.com/terms/s/seedcapital.asp

Linders, Ben. “Interview with Capers Jones on Measuring for Agile Adoption. InfoQ. May 30, 2013. https://www.infoq.com/articles/Jones-measuring-agile-adoption/

National Institute of Standards and Technology. “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities” (NIST SP 800-218). NIST Computer Security Resource Center website. February 2022. https://csrc.nist.gov/pubs/sp/800/218/final

Office of the Secretary of Defense. “Continuous Authorization To Operate (cATO)” (Memorandum for Senior Pentagon Leadership Defense Agency and DoD Field Activity Directors). Department of Defense website. February 3, 2022. https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF

Office of the Under Secretary of Defense for Acquisition and Sustainment. “Budget Activity (BA) ‘BA-08’: Software and Digital Technology Pilot Program Frequently Asked Questions.” U.S. Department of Defense. September 28, 2020. https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Budget%20Activity%20-%20BA-08.pdf

Office of the Under Secretary of Defense. “Public-Private Talent Experience.” OUSD Human Capital Initiatives website. October 3, 2024 [accessed]. https://www.hci.mil/ppte.html

Perez, Lisbeth. “Hicks Orders Reuse/Reciprocity Changes to Quicken ATO Process.” MeriTalk. May 9, 2024. https://www.meritalk.com/articles/hicks-orders-reuse-reciprocity-changes-quicken-ato-process/

Secretary of the Army. “Army Directive 2024-02 (Enabling Modern Software Development and Acquisition Practices)” (memorandum). March 11, 2024. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN40433-ARMY_DIR_2024-02-000-WEB-1.pdf

Software Factory Coalition. SFC Home Page. SFC website. June 30, 2024 [accessed]. https://coalition.dso.mil

U.S. Army Public Affairs. “Army announces new policy to drive adoption of agile software development practices.” U.S. Army Website. March 9, 2024. https://www.army.mil/article/274356/army_announces_new_policy_to_drive_adoption_of_agile_software_deveopment_practices

U.S. Senate Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform. “Recommendations for Inclusion in the Appropriations Bill or National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2025.” Commission on PPBE Reform website. October 1, 2024 [accessed]. https://ppbereform.senate.gov/wp-content/uploads/2024/04/ConsolidatedLegLanguageforFY25_Final.pdf

White House. “Executive Order on Improving the Nation’s Cybersecurity” (Executive Order 14028). White House website. May 12, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

Glossary

Term	Definition
Artifact Repository	An artifact repository is a system for storage,retrieval, and management of artifacts and their associated metadata. Note that programs may have separate artifact repositories to store local artifacts and released artifacts. It is also possible to have a single artifact repository and use tags to distinguish the content types.
CI/CD Pipeline	The process workflows and associated tools to achieve the continuous integration and continuous deployment of software with maximum use of automation.
Code	Software instructions for a computer,written in a programming language. These instructions may be in the form of either human-readable source code, or machine code, which is source code that has been compiled into machine executable instructions.
Container	A standard unit of software that packages up code and all its dependencies, down to, but not including the OS. It is a lightweight,standalone, executable package of software that includes everything needed to run an application except the OS: code, runtime,system tools, system libraries and settings.
Continuous Authority to Operate	cATO is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system's cyber posture.
Continuous Build	Continuous build is an automated process to compile and build software source code into artifacts. The common activities in the continuous build process include compiling code, running static code analysis such as code style checking, binary linking (in the case of languages such as C++), and executing unit tests. The outputs from continuous build process are build results,build reports (e.g., the unit test report, and a static code analysis report), and artifacts stored into Artifact Repository. The trigger to this process could be a developer code commit or a code merge of a branch into the main trunk.
Continuous Integration	Continuous integration goes one step further than continuous build. It extends continuous build with more automated tests and security scans. Any test or security activities that require human intervention can be managed by separate process flows. The automated tests include, but are not limited to, integration tests, a system test,and regression tests. The security scans include, but are not limited to, dynamic code analysis, test coverage, dependency/BOM checking, and compliance checking. The outputs from continuous integration include the continuous build outputs, plus automation test results and security scan results. The trigger to the automated tests and security scan is a successful build.
Continuous Delivery	Continuous delivery is an extension of continuous integration to ensure that a team can release the software changes to production quickly and in a sustainable way. The additional activities involved in continuous integration include release control gate validation and storing the artifacts in the artifact repository, which maybe different than the build artifact repository. The trigger to these additional activities is successful integration, which means all automation tests and security scans have been passed. The human input from the manual test and security activities should be included in the release control gate. The outputs of continuous delivery are a release go/no-go decision and released artifacts, if the decision is to release.

Term	Definition
Continuous Monitoring	Continuous monitoring is an extension to continuous operation. It continuously monitors and inventories all system components, monitors the performance and security of all the components, and audits &logs the system events.
Control Gate	A control gate is a point in the software lifecycle process when the code is evaluated, and a decision is made to proceed or stop progress. Control gates can contain automated and manual checks.
Delivery	The process by which a released software is placed into an artifact repository that operational environment can download.
Deployment	The process by which the released software is downloaded and deployed to the production environment.
DevSecOps	DevSecOps is a combination of software engineering methodologies, practices, and tools that unifies software development(Dev), security (Sec), and operations (Ops). It emphasizes collaboration across these disciplines, along with automation and continuous monitoring to support the delivery of secure, high-quality software. DevSecOps integrates security tools and practices into the development pipeline,emphasizes the automation of processes,and fosters a culture of shared responsibility for performance, security, and operational integrity throughout the entire software lifecycle, from development to deployment and beyond.
Infrastructure as-code	The management of infrastructure (networks, virtual machines, load balancers,and connection topology) in a descriptive model, using the same versioning that the DevSecOps team uses for source code. Infrastructure as Code evolved to solve the problem of environment drift in the release pipeline.
Iron Bank	Holds the hardened container images of DevSecOps components that DoD mission software teams can utilize to instantiate their own DevSecOps pipeline. It also holds the hardened containers for base operating systems, web servers, application servers,databases, API gateways, message busses for use by DoD mission software teams as a mission system deployment baseline. These hardened containers, along with security accreditation reciprocity, greatly simplifies and speeds the process of obtaining an Approval to Connect (ATC) or Authority to Operate (ATO).
Repository	A central place in which data is aggregated and maintained in an organized way.
Software Factory	A software factory is defined as a collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.
Software Supply Chain	The software supply chain is a collection of steps that create, transform, and assess the quality and policy conformance of software artifacts. (NIST SP 800-204D)
Mission-Critical Platforms Software Factory	This type of software factory focuses 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.
Training and Education Software Factory	A type of software factory that is dedicated to training military personnel in software development and continuous integration/continuous delivery (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.

Term	Definition
Innovation Pipeline Software Factory	A type of software factory that acts as a conduit 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.
IaC and CI/ CDSoftware Factory	A type of software factory that is 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.
Platform One	Platform One is a Department of the Air Force organization that provides open-source tools and enterprise solutions for teams to build, deploy, and secure better software at scale. Platform One supports both the teams buying technology and the warfighters using it, providing the tools and infrastructure they need to build, launch,and manage secure software.
Refactoring	Refactoring is defined as restructuring software to improve its quality without altering its external behavior.
Zero Trust	Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element,node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses. The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.3Page 4Platform One Platform One is a Department of the Air Force organization that provides open-source tools and enterprise solutions for teams to build, deploy, and secure better software at scale. Platform One supports both the teams buying technology and the warfighters using it, providing the tools and infrastructure they need to build, launch,and manage secure software.

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA