Statement of
**Dr. Daniel Patt**
Senior Fellow
The Hudson Institute

Before the

House Committee on Armed Services Subcommittee on Cyber, Information Technologies, and Innovation

on

# "Too Critical to Fail: Getting Software Right in an Age of Rapid Innovation"

March 13, 2024

## Introduction

Chairman Gallagher, Ranking Member Khanna, and distinguished Members of the Subcommittee on Cyber, Innovative Technologies, and Information Systems (CITI), thank you for the opportunity to testify today on the critical role of software in the Department of Defense (DoD) and how we can harness its power to drive innovation adoption and achieve military advantage.

My name is Dr. Daniel Patt, and I am a Senior Fellow at the Hudson Institute, where I study the intersection of technology, innovation, and national security. While I am here in an individual capacity, my breadth of roles offers me a unique perch – I get to see inside a broad array of commercial companies, especially in robotics, the exciting world of applied AI, and enterprise software. I also get a window into high end national security technology to counter emerging threats at STR. I'm a co-founder and former CEO of an industrial robotics company, and I had the privilege of serving in a variety of roles at the Defense Advanced Research Projects Agency (DARPA), where I launched the Mosaic Warfare initiative, and I am a veteran of aerospace startup outfits and big aerospace alike. These experiences have given me a unique perspective on the challenges and opportunities facing the DoD as it seeks to modernize its software acquisition and development practices.

The topic of today's hearing could not be more timely or important. Software is now ubiquitous in every aspect of modern warfare, from the systems that power our weapons platforms and command and control networks, to the tools that enable our intelligence analysts and logisticians to do their jobs more effectively. As the DoD seeks to maintain its military advantage in an era of great power competition, its ability to develop, acquire, and deploy cutting-edge software capabilities will be a key determinant of success. Even as we hear about Artificial Intelligence (AI), and its coming impact on the economy and national security, remember that every AI capability depends on a robust ability to deploy and update software. **We can't lead in AI if we don't get software right.**

Yet, despite the central role that software plays in modern defense, the DoD's mainstream approach to software acquisition and development is simply not up to the task. As the Government Accountability Office (GAO) has repeatedly documented, the DoD's software programs are often plagued by obsolete practices, plodding delivery, and performance shortfalls. These challenges are not simply a matter of technical complexity or resource constraints, but rather a reflection of deep-seated structural and cultural barriers that prevent the DoD from leveraging the full potential of software innovation.

In my testimony today, I will argue that overcoming these barriers and unleashing the power of software for military advantage will require a fundamental shift in the way the DoD approaches software acquisition and development. Specifically, I will make the case for prioritizing adaptability as the key driver of software innovation in the DoD, and for focusing on two key enablers of adaptability: **(1) the ability to deploy and update software quickly via continuous authority to operate or cATOs and ATO reciprocity**, and **(2) the increased availability of qualified technical expertise to guide the DoD's software efforts through easier term hiring authority.**

By embracing adaptability as the cornerstone of its software strategy, and by investing in the tools, processes, and people needed to enable it, the DoD can position itself to harness the full potential

of software innovation and maintain its military advantage in the face of an increasingly complex and dynamic threat environment. The stakes could not be higher – and the time for action is now.

## The Imperative for Adaptability in Strategic Competition

As the United States finds itself engaged in a long-term strategic competition with the People's Republic of China, it is crucial to recognize that military dimensions of this long-term competition depend on the DoD engaging in evolution – advancing in move-counter-move cycles, day after day, year-after-year. Our success hinges on our ability to adopt and adapt technology rapidly in response to evolving threats and opportunities. In this competition, the nation that can harness data and technology to quickly assemble, deploy, and continually update its military capabilities will hold a decisive advantage. And because essentially every US system – military and commercial – is powered by software, this means that **an upper hand in strategic competition means getting software right.**

It's essential to understand the dual nature of software: fluid and frozen. During development, software is fluid— like wet potter's clay, it can be molded and adapted quickly by programmers adding new features, fixing bugs, and optimizing performance. However, once the software is compiled and deployed, it becomes brittle and frozen—inflexible only able to run on specific hardware configurations, severed from its source code and development environment.

Regrettably, the Department of Defense's current approach to software development and acquisition largely treats software as a frozen, finished product. This mindset is exemplified by the F-35 Joint Strike Fighter program, which remains locked in a mostly waterfall development cycle for its core operational software. The process of planning, testing, and delivering a new software block can take years, as evidenced by the lengthy progression from Block 3 to 3B to Block 4[1]. While the capabilities delivered may be impressive, this drawn-out process severely hinders our ability to adapt to emerging threats or seize fleeting opportunities for tactical advantage. This is software done wrong – brittle, frozen, and forcing an unadaptable force.

Once a conflict begins, adaptability and scaling drive outcomes. We must seize the current moment to prepare. For examples about how conflict drives adaptation, consider that the lifecycle of a radio in Ukraine is only about 3 months before it needs to be reprogrammed or swapped out as the Russians optimize their electronic warfare against it. The peak efficiency of a new weapon system is only about 2 weeks before countermeasures emerge. As another example of superior weapons systems handicapped by lack of software adaptability, consider that Excalibur precision artillery rounds initially had a 70% efficiency rate hitting targets when first used in Ukraine. However, after 6 weeks, efficiency declined to only 6% as the Russians adapted their electronic warfare systems to counter it[2]. This shows how quickly adversaries can adapt to new technologies. This lack of adaptability is not an inherent property of software but rather a consequence of how we

[1] Consider the delays in Technology Refresh 3 (TR-3), the crucial enabler for Block 4 modernization, providing the necessary computational power. However, its delivery faced delays due to challenges in hardware and software development and the testing of the Integrated Core Processor (ICP) – documented in the December 2022 Selected Acquisition Report (SAR) for the F-35

[2] This and other examples from the conflict in the Ukraine are sourced from Dr. Jack Watling, Royal United Services Institute (RUSI), who is a leading scholar on technological trends in land warfare

choose to manage it. After all, Ukrainian units with organic programming capability to rapidly adapt their UAV software have about 50% efficiency, while those reliant on companies and longer supply chains to make changes struggle to hit 20% efficiency. Keeping software in a pliant, fluid state is the only way to maintain tactical innovation.

Encouragingly, there are a handful of leaders inside the Department who are pioneering the kinds of practices the US needs to compete, and we can draw lessons from their success. To exploit the fluid nature of software and unlock its potential for rapid adaptation, the Department of Defense must embrace a fundamentally different approach. This approach should be guided by key principles: (i) lower the barriers to entry to get software on operational systems and networks, (ii) open up access to the Department's vast troves of data by exposing system interfaces, and (iii) let a larger swath of partners and industry players get on contract and use this. By removing bureaucratic barriers, the DoD can foster a culture of innovation and agility, and possibly unleash a new industrial base.

To truly harness the power of software for adaptive military advantage, the DoD must go beyond isolated successes and drive systemic change. Every leader across the Department should have a plan for implementing these principles. This change starts with recognizing that software is not just an enabler but a central pillar of modern warfare. Getting it right is not an option, it's a mandate. By prioritizing investments in software development, data access, talent, and infrastructure, the United States can position itself to outpace and outmaneuver its competitors in the years ahead. The alternative—continuing to treat software as a static, secondary consideration—risks ceding the initiative and falling behind in this critical domain.

## Challenges and Roadblocks

While the imperative for software adaptability is clear, the Department of Defense faces a range of challenges and roadblocks that hinder its ability to achieve this vision. These obstacles span the lifecycle of software development, from initial deployment to ongoing testing and acquisition, and are deeply rooted in the DoD's organizational culture, processes, and workforce. Years after the Defense Innovation Board (DIB) made key recommendations to the Department, implementation remains slow and incomplete[3]. Top-level Department policy documents remain dreadfully out-of-date, not accommodating incremental refinement approaches[4].

One of the most significant challenges is the difficulty in deploying, testing, and acquiring software in a timely and efficient manner. The DoD's current Authority to Operate (ATO) process is a prime example of this struggle. Intended to ensure the security and reliability of software systems, the ATO process has instead become a bureaucratic bottleneck that slows down the deployment of new capabilities and stifles innovation, and can aggravate security problems[5]. The process often involves lengthy reviews and documentation requirements that can take months or even years to

[3] See GAO report, GAO-23-105611

[4] See GAO report, GAO-23-105867, Table 4

[5] For example, ATOs focus on obtaining system authorizations but fall short in implementing continuous monitoring of risk once authorization is reached – See DoD memorandum for senior pentagon leadership, subject: Continuous Authorization To Operate (cATO), signed by David W. McKeown

complete, by which time the software may already be outdated or no longer meet evolving mission needs.

Moreover, the ATO process has unintentionally created a new form of vendor lock-in, where companies that have successfully navigated the arduous process can use their ATO as a barrier to entry for competitors. This lock-in effect stifles competition and hinders the DoD's ability to tap into the latest innovations from across the commercial sector. Smaller, more agile companies with cutting-edge software solutions may be deterred from working with the DoD altogether due to the time and resource demands of the ATO process. Perhaps most shockingly, DOD lacks ATO reciprocity within and between programs, services, and agencies, hindering the sharing of software platforms and rapid integration of capabilities[6], which means that long timelines aren't a one-time obstacle, they repeat over and over.

Another major roadblock is the DoD's struggle to allocate resources effectively and respond quickly to evolving software needs. The Department's budgeting and acquisition processes are still largely geared towards traditional hardware programs, with rigid requirements and long lead times. This mismatch makes it difficult for software development teams to secure the funding and support they need to iterate rapidly and deliver capabilities in a timely manner. As a result, promising software initiatives may languish or fail to scale, while legacy systems continue to consume a disproportionate share of resources.

Compounding these challenges is a severe talent deficit within the DoD's software workforce. The Department struggles to attract and retain top digital talent, as it competes with the private sector for a limited pool of skilled professionals. The Department has failed to establish a cadre of high-end digital talent[7]. Government hiring processes can be slow and cumbersome, and the DoD's bureaucratic culture and rigid career paths may strip away the job autonomy needed to recruit talented technical leaders. This talent gap leaves the DoD without the in-house expertise needed to effectively manage software programs, make informed technical decisions, and drive innovation.

Finally, there are persistent misconceptions and knowledge gaps within the DoD around key software concepts such as data rights, interface rights, and the appropriate role of industry in the software innovation process. These misunderstandings can lead to suboptimal contracting strategies, intellectual property disputes, and a lack of effective collaboration between government and industry stakeholders. For example, the DoD may pursue a strategy of seeking to own all software source code, rather than focusing on owning the right APIs and interfaces to ensure interoperability and avoid vendor lock-in[8].

Addressing these challenges and roadblocks will require a concerted effort from DoD leadership, policymakers, and industry partners. It will involve streamlining bureaucratic processes, updating acquisition strategies, investing in workforce development, and fostering a culture of experimentation and calculated risk-taking. While daunting, these reforms are essential if the DoD

---

[6] See GAO report, GAO-23-105611, and also Defense Innovation Board, Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage

[7] See GAO report, GAO-23-105611, "it has yet to establish a cadre of software developers"

[8] See, for example, 2021 National Defense Authorization Act, Sec. 804, which mandates exposed system interfaces and extends the pre-existing Modular Open Systems Architecture (MOSA) law

is to harness the full potential of software for adaptive military advantage in an era of great power competition.

## Promising Developments and Best Practices

Amidst the challenges and roadblocks faced by the Department of Defense in its pursuit of software adaptability, there are also reasons for optimism. In recent years, the DoD has taken important steps to improve its software acquisition and development practices, and pockets of excellence have emerged across the services that offer valuable lessons and models for success.

One of the most significant developments has been the establishment of the Adaptive Acquisition Framework (AAF) by fellow witness and former Under Secretary of Defense for Acquisition and Sustainment, Ellen Lord. The AAF represents a major shift in the DoD's approach to acquisition, moving away from a one-size-fits-all model towards a more flexible, tailored approach that recognizes the unique characteristics of software. The framework includes a dedicated software acquisition pathway, as promoted by the FY2020 NDAA, which emphasizes the use of modern development practices, including DevSecOps[9], and encourages greater collaboration between government and industry.

The AAF is a crucial step in the right direction, but its impact will depend on how effectively it is implemented across the DoD. To date, the adoption of the framework has been uneven, with some organizations moving quickly to embrace its principles and others lagging behind. It will be important for DoD leadership to continue to prioritize and incentivize the use of the AAF, and to provide the necessary resources and support to enable its success.

Encouragingly, there are pockets of excellence within the DoD where forward-leaning leaders are already putting these principles into practice. The Navy's PEO Digital is restructuring its portfolio to deliver on modern metrics like adaptability, resilience, time lost, and cost per user. The Navy's PEO IWS is similarly leading the way – having stood up a software factory[10], working a continuous authority to operate (cATO), opening up systems interfaces, implementing Modular Open Systems Architecture (MOSA)[11] acquisition models, using digital twins to enable federated software development, and pioneering a portfolio management approach across its more than 140 constituent programs. PEO IWS is the poster-child for why resourcing flexibility – like that delivered by BA-08[12], the recommendations of the PPBE commission[13] around colors of money, or portfolio

[9] DevSecOps is the integration of security, software development, and software operations into a continuous cycle, with security baked in as a forethought, and feedback from operations informing development priorities

[10] See, for example: https://federalnewsnetwork.com/navy/2023/10/several-navy-peos-put-personnel-first-in-modernization-efforts/

[11] See https://www.dau.edu/acquipedia-article/modular-open-systems-approach-mosa

[12] As recommended by the DIB SWAP study: Budget Activity (BA) "BA-08": Software and Digital Technology Pilot Program https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Budget%20Activity%20-%20BA-08.pdf

[13] See recommendation #11 "Recommendation #11 (Key). Address Challenges with Colors of Money "which is found in Section V, https://ppbereform.senate.gov/wp-content/uploads/2024/03/Commission-on-PPBE-Reform_Full-Report_6-March-2024_FINAL.pdf

management – is essential to adaptability in combat capability[14]. Bit by bit, the Navy is moving closer to something like the App Store model for deployment – for example PMW 150 oversaw the first ever over the-air installation of a Software element of a major acquisition program to a US navy ship in FY23, followed weeks later by first over-the-air update, providing new capability to that same ship, and multiple installs on additional ships[15]. While the progress looks humble to begin with, I have hope that we can build up from this.

Over in the Air Force, the original Advanced Battle Management System (ABMS) got off to a rough start, focusing more on demonstrations than solving the underlying problems associated with building and evolving modern battle networks[16]. But in recent years, the ABMS Cross-Functional Team has demonstrated a modern approach to requirements for adaptable capability, with well-vetted top-level needs, and continuous measurement for assessing progress, but being careful not to over-specify solutions. On the execution side, PEO C3BM is pioneering a more adaptable way to build out complex battle networks and decision aids. It has invested in accredited digital infrastructure, and takes a modular approach, for example Tactical Operation Centers-Light (TOC-L) kits are being deployed as a "basic building block" for command and control (C2) infrastructure. The goal is to deploy simple, proven technologies first, starting from a foundational level, then iterate and scale up to more complex capabilities over time, allowing faster adaptation to operational needs[17]. This is taking a clue from Gall's Law[18] – a principle from systems theory which suggests that complex systems that work are invariably found to have evolved from simpler systems that worked.

Inside OSD, the Deputy Assistant Secretary of Defense for Acquisition Integration and Interoperability (AI2) in the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) is leading by example, demonstrating how to quickly implement the software acquisition pathway for joint programs, using the AAF for evolving requirements alongside development, facilitating faster delivery of capabilities to warfighters[19]. The Army, through its deputy assistant secretary of the Army for strategy and acquisition reform, is also trying to overhaul how it develops and deploys software, as indicated by its release this week of a new policy Enabling Modern Software Development and Acquisition Practices, which, like the USAF ABMS effort,

---

[14] Consider PPBE commission report, Section V: “It is very difficult to predict the exact ratio of RDT&E and O&M funding that will be required when building the budget, due to the unforeseen challenges that arise in the development and sustainment of a business system. In FY 2023, a software patch was needed to address technical issues on the program. Financial managers and fiscal attorneys spent considerable time assessing and determining which parts of the patch represented a true upgrade in capability (RDT&E funded) vice basic sustainment (O&M funded), even though there is no such distinction to the software developer. A realignment of funding was required to fully fund the software patch, creating execution delays and further pressure on the program since O&M funds would soon be expiring.”

[15] https://www.peoc4i.navy.mil/Portals/98/Documents/Tear-Sheets/2023_PMW%20150_Tear%20Sheet.pdf?ver=VTpy7S0zRS6ePS1wbIcdJw%3D%3D

[16] See, for example, https://www.defensenews.com/air/2021/08/19/new-us-air-force-secretary-to-shake-up-advanced-battle-management-program/ or https://www.gao.gov/products/gao-20-389

[17] See, for example, https://defensescoop.com/2024/02/14/air-force-cropsey-c3bm-c2-budget/ and https://www.airandspaceforces.com/daf-battle-network-contribution-jadc2/ and https://www.afcea.org/signal-media/technology/illuminating-department-air-force-battle-network

[18] https://www.amazon.com/Systemantics-Systems-Work-Especially-They/dp/0812906748

[19] https://www.ndia.org/events/2023/12/11/hudson-joint-integration

pushes to change the way requirements are written, favoring high-level needs statements and concision over hyper-specific direction, and explicitly recognizes that sustainment can be a vibrant and innovative phase of a system's lifecycle, with new features and functionality driving enhanced capability.

These examples demonstrate that it is possible for the DoD to achieve significant improvements in capability adaptability through keeping software fluid and allowing software developers and systems to refine their work based on feedback from operational systems, even within the constraints of the current system. By embracing modern development practices, fostering close collaboration with industry, and empowering software teams to iterate rapidly, these organizations have been able to deliver real value to the warfighter at a pace that would have been unthinkable just a few years ago.

Looking ahead, it will be important for the DoD to build on these successes and scale them across the enterprise. This will require continued leadership and investment in software innovation, as well as a willingness to experiment with new models and approaches. It will also require a concerted effort to capture and share best practices across the DoD, so that successful models can be replicated and adapted to meet the unique needs of different organizations and mission areas.

By learning from these promising developments and best practices, the DoD can begin to chart a path towards a more adaptable, software-driven future. While the challenges are significant, the potential benefits – in terms of increased agility, responsiveness, and operational effectiveness – are simply too great to ignore.

## Key Recommendations

To overcome the challenges and build on the promising developments in software adaptability, the Department of Defense must take bold action across several key areas. The following recommendations are designed to address the most pressing needs and opportunities for reform, and to accelerate the DoD's progress towards a more agile, software-driven future.

### a. Enable rapid deployment and updating of software

The DoD must prioritize efforts to streamline the software deployment process and enable more rapid updating of software capabilities in the field. A key part of this effort will be to reform the ATO process, moving from a static, compliance-based model to a continuous, risk-based approach. This will require close collaboration between software development teams, cybersecurity experts, and operational commanders to ensure that software is deployed quickly and securely, while also meeting mission needs. In particular, the Department should:

**Establish a DoD-Wide Continuous ATO (cATO) Framework**: Implement cATO framework and guidance across the DoD to enable real-time, risk-based decision-making. This approach should automate the authorization process, leveraging standardized security controls and practices, significantly reducing deployment timelines for new and updated software capabilities

**Create mechanisms for ATO reciprocity** within and between programs, services, and other DoD agencies. This would enable the sharing of software platforms, components, and infrastructure, facilitating rapid integration of capabilities across platforms and services. Consider employing a

centralized repository for ATO artifacts at CIO, with access rules enabling services to utilize existing ATOs where applicable.

## b. Attract and empower top technical talent

To drive software innovation and adaptability, the DoD must attract and retain top technical talent from across industry and academia. You can outsource the coding, but you can't outsource all of the thinking or competence. This will require a multi-faceted approach that includes reforming the hiring process, making sure they have autonomy in their roles, creating more flexible career paths, and providing opportunities for continuous learning and development.

The Department of Defense can compete and hire great talent. Having come from DARPA, I believe there is great value in the "Tour of Duty" approach, which brings in top tech talent for periods of time, where they can contribute to specific projects. This creates a strong motivation to have an impact before their clock runs out. The fluidity between private and public sectors also brings in fresh perspectives and familiarity with commercial trends.

Much of this can be accomplished by **expanding existing authorities**. The DoD should widely adopt term appointments like HQE positions, and hold HR organizations accountable for responsive hiring timelines. Organizations should be empowered to **temporarily convert some permanent billets to term positions**, using tools like to DARPA's 10 U.S.C. § 1109 "Direct hire authority" to encourage personnel rotation.

HR organizations across the Department should **overhaul performance evaluation** and promotion criteria for digital and technical roles to reward rapid delivery, user impact, experimentation and continuous improvement rather than just compliance with bureaucratic processes. Create fast-track promotion opportunities for high performers[20].

## c. Prioritize APIs and data accessibility

To enable greater software adaptability, enable composition of new tactics and operational concepts, unlock the power of data, and accelerate the development of AI capabilities, the DoD must prioritize exposing the APIs and interfaces of its existing systems, and requiring, in accordance with the law, that these be made. DoD can no longer treat software like a hardware deliverable, and must embrace the fact that each component is part of a larger ecosystem of interacting elements. This will unleash a new industrial base create the foundation for innovation in AI and machine learning applications. Specifically, the DoD should:

- Establish clear guidance and best practices for API development and management, with a focus on exposing interfaces, and widely distributing them. Propagate this guidance to PEOs, PMs, and contracting officers.
- Publish comprehensive data catalogs that document key DoD data sources, data types, schemas, and APIs. These catalogs should be made available via platforms like Advana to qualified users across the DoD, industry, and research community.

[20] Consider the recommendations of Jennifer Pahlka in "Recoding America"

- Stand up one or more centralized repositories for key interfaces, associated documentation, and reference implementations. These "interface repositories" explicitly called for in Section 804 of the FY21 NDAA, and yet never implemented.
- Work with industry partners to ensure that critical interfaces are well-documented, secure, and scalable to enable continuous evolution and integration.

### d. Embrace a diverse, software-centric industrial base

Finally, the DoD must work to foster a more diverse, software-centric industrial base that can support its needs for adaptable, innovative software capabilities. Our future industrial base needs won't be met by adding one more prime contractor. We need to tap into a diverse base of hundreds or thousands of companies that have specialized capabilities that can be brought to bear.

By embracing these recommendations and committing to a sustained effort to drive change, the DoD can position itself to harness the full potential of software for adaptive military advantage. While the challenges are significant, the imperative for action is clear – and the benefits, in terms of increased agility, innovation, and operational effectiveness, are simply too great to ignore.

## Conclusion

The United States stands at a critical juncture in its pursuit of military superiority in an era of strategic competition. While we possess the world's most formidable military today, our current approach to software development and acquisition threatens to undermine that advantage. As I have outlined in my testimony and in my prior work on "Software Defines Tactics," the ability to rapidly adapt and evolve software is not just an enabler of military capabilities—it is the foundation of military advantage itself in the digital age.

The stakes could not be higher. If we fail to transform our approach to software, we risk ceding the advantage to our adversaries and losing the ability to compete effectively in the long-term strategic competition ahead. But if we embrace the power and fluidity of software, empower our workforce, and build the technical and institutional foundations for adaptability, we have the opportunity to out-innovate, out-adopt, out-scale, and out-compete would-be aggressors for decades to come. I urge this committee and this Congress to seize this moment and to champion the oversight and reforms necessary to secure our military advantage through software. The time for action is now.

## Appendix

For additional detail, interested readers are referred to:
Jason Weiss and Dan Patt, "**Software Defines Tactics**: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era", The Hudson Institute, December 2020
https://s3.amazonaws.com/media.hudson.org/Software+Defines+Tactics.pdf