Revision and Codification of Software Acquisition Pathways - Section 318 Analysis

<Generated by Gemini Deep Research>

Key Points

Section 318 of the FoRGED Act (Senate Bill 5618) mandates the establishment of specific software acquisition pathways within the Department of Defense. This provision aims to streamline the acquisition, development, integration, and timely delivery of software and related hardware. It codifies at least two pathways: one for applications and another for embedded systems. Key requirements include the use of proven technologies, rapid capability demonstration (within one year), and continuous updates (at least annually). Software acquired under these pathways will not be treated as a Major Defense Acquisition Program (MDAP). The Secretary of Defense is directed to use a risk-based approach for innovative technologies and to implement an expedited process with streamlined requirements, budget, and acquisition processes. The provision explicitly exempts software acquisition under these pathways from the Joint Capabilities Integration and Development System Manual and Department of Defense Directive 5000.01. It mandates tailored policies and processes for various elements of acquisition, including user needs, prioritization, user engagement, acquisition strategies, contracting, iterative development, and cybersecurity. Section 318 repeals Section 800 of the National Defense Authorization Act for Fiscal Year 2020, which was a precursor to this codification.

History of the recommendation

The impetus behind Section 318 stems from a widely acknowledged need to modernize the Department of Defense's approach to software acquisition. There is a recognition that the Department risks falling behind adversaries who can more effectively leverage rapid technological advancements due to outdated and bureaucratic processes that have historically slowed the delivery of cutting-edge software to warfighters [1]. These slow processes have left critical Department systems potentially vulnerable. The increasing centrality of software in modern warfare and defense capabilities necessitates a fundamental shift in how the DoD procures and deploys digital tools. Traditional, hardware-centric acquisition timelines and procedures are ill-suited to the rapid iteration and evolution inherent in software development [1]. This growing disparity between the pace of technological change and the speed of defense acquisition highlights the urgency for reform.

While Senate Bill 5618 was introduced in late 2024 [4], the concepts embodied in Section 318 had been gaining traction within the Department of Defense. For instance, a memo issued by Defense Secretary Pete Hegseth in March 2025, although part of a hypothetical future scenario, directed the adoption of the Software Acquisition Pathway (SWP) as the preferred method for software procurement [1]. This directive underscores the executive branch's recognition of the critical need for faster and more efficient software acquisition processes to maintain a technological advantage [1]. The fact that such a directive was deemed necessary suggests a pre-existing understanding within DoD leadership of the shortcomings of the traditional acquisition framework when applied to software.

The establishment of specific software acquisition pathways is not an entirely novel concept within the DoD. Prior to the FoRGED Act, the Software Acquisition Pathway (SWP) was authorized under Section 800 of the National Defense Authorization Act for Fiscal Year 2020 [2]. Section 318 of the FoRGED Act explicitly repeals this earlier legislative provision [4]. This repeal indicates a legislative intent to supersede and potentially refine the previous guidance on software acquisition pathways, suggesting a move towards a more permanent and potentially more detailed legal framework within Title 10 of the United States Code. The decision to codify these pathways within the main body of law rather than as a note to the code signifies a higher level of commitment and permanence for this approach to software acquisition.

The Defense Innovation Unit (DIU) and its pioneering Commercial Solutions Opening (CSO) process have likely played a significant role in shaping the concepts within Section 318. DIU's success in demonstrating faster and more flexible acquisition methods, often working with non-traditional vendors, has provided a model for reform [1]. The rapid progress of projects like the Replicator software project, which moved from problem statement to contract award in a significantly shorter timeframe than traditional acquisitions [1], and DIU's overall track record in awarding Other Transaction Authorities (OTAs) to innovative companies [1] likely demonstrated the viability and benefits of more agile acquisition approaches. The emphasis in Section 318 on rapid prototyping, leveraging commercial innovation, and the implicit endorsement of tools like OTAs and CSOs through its streamlined processes suggests an institutionalization of these successful models.

Furthermore, the Government Accountability Office (GAO) has consistently advocated for the modernization of DoD software acquisition practices, emphasizing the need for iterative development methodologies and better alignment with leading commercial practices [12]. GAO reports have highlighted the challenges the DoD faces in acquisition speed and innovation, noting that some acquisition pathways lack the iterative processes necessary for rapid weapons system development [14]. DOD Instruction 5000.87, issued in October 2020, had already established the software pathway [2]. Section 318 can be viewed as a legislative reinforcement and strengthening of these existing administrative efforts within the Department. The codification of these pathways in law provides a more robust mandate and aims to ensure greater consistency and permanence across the entire Department of Defense, making these reforms less susceptible to future policy shifts.

Desired Effect of the recommendation

A primary objective of Section 318 is to significantly accelerate the delivery of software capabilities to warfighters, thereby reducing the often lengthy timeframes associated with traditional acquisition processes [1]. The provision's explicit requirement for demonstrating the viability of new software within one year of funding obligation, coupled with the mandate for annual updates, directly addresses the critical need to overcome the slow pace of traditional acquisition and provide timely software solutions to meet evolving operational demands. This emphasis on speed recognizes the dynamic nature of software as a capability that requires frequent updates and adaptations to remain effective.

By enabling the faster and more efficient delivery of modern software, Section 318 intends to enhance the lethality and overall effectiveness of military systems and personnel [1]. In contemporary defense, software is increasingly central to maintaining a competitive edge against potential adversaries. The rapid deployment of advanced software can lead to improved decision-making, enhanced situational awareness, and more effective weapon systems. Therefore, the ability to acquire and field cutting-edge software swiftly is not merely a matter of process improvement but a strategic imperative for ensuring the military possesses the necessary tools to succeed in its missions.

Section 318 is designed to foster greater agility and adaptability in software acquisition by aligning with modern software development practices such as Agile and DevSecOps [5]. These methodologies emphasize iterative development, continuous feedback from users, and the integration of security considerations throughout the development lifecycle. This shift away from traditional waterfall development models acknowledges the importance of flexibility and collaboration in producing software that effectively meets user needs and can adapt to changing requirements and threats. The formal incorporation of these practices into acquisition pathways through Section 318 aims to create a more responsive and adaptive software development ecosystem within the DoD.

The provision also seeks to increase the Department of Defense's ability to leverage innovation from the commercial sector [1]. By streamlining acquisition processes and potentially lowering barriers to entry, Section 318 aims to make it easier for non-traditional vendors, who are often at the forefront of software innovation, to work with the DoD. The repeal of restrictive guidance further supports this objective. This focus on commercial solutions recognizes that the commercial sector frequently leads in software development, and facilitating the adoption of these cutting-edge technologies is crucial for maintaining a technological advantage in defense.

While not explicitly framed as a separate benefit in the user's prompt, Section 318(h)(7) mandates ensuring the delivery of cyber-secure systems. This underscores the intent to build security into the software acquisition process from its inception [1]. Given the escalating sophistication of cyber threats, guaranteeing the security of defense software is of paramount importance. By including this as a key element in the implementation of the software acquisition pathways, Section 318 aims to proactively prevent vulnerabilities and safeguard critical defense systems.

Feature	**Traditional Acquisition**	**Section 318 Pathways**
Timeline	Often multi-year, hardware-centric	Target of under one year for minimum viable product
Requirements Process	Detailed upfront requirements (JCIDS Manual)	Streamlined, iterative, based on user feedback
Development Approach	Often Waterfall	Agile, DevSecOps emphasized
Vendor Engagement	Primarily traditional defense contractors	Encourages non-traditional, commercial vendors (CSOs, OTAs)
Regulatory Framework	Subject to DOD Directive 5000.01 and JCIDS Manual	Exempt from DOD Directive 5000.01 and JCIDS Manual

Treatment as MDAP	Often treated as Major Defense Acquisition Program	Generally not treated as MDAP

Potential Negative impacts of the recommendations

The Department of Defense's acquisition system is characterized by its substantial size and intricate procedures. Implementing the streamlined pathways introduced by Section 318 may encounter resistance to change and difficulties in adapting existing processes [18]. Effectively training DoD personnel on these new processes will be essential but could face significant organizational hurdles. The established nature of the acquisition bureaucracy presents an inherent inertia that could impede the smooth adoption of these new methodologies. Overcoming deeply ingrained habits and bureaucratic obstacles will necessitate focused effort and strong leadership commitment.

While a stated goal of Section 318 is to enhance cybersecurity, the emphasis on rapid development and deployment could inadvertently lead to compromises in security testing and implementation if not carefully managed [1]. Achieving a balance between the desired speed of delivery and the necessity of robust cybersecurity will be a critical challenge. An expedited acquisition process might inadvertently prioritize speed over thorough security reviews and testing. Ensuring that cybersecurity is integrated from the initial stages of development, as intended by the "DevSecOps" approach, will require diligent attention and the appropriate expertise at every phase of the software lifecycle.

The streamlined requirements process outlined in Section 318, while intended to accelerate acquisition, carries the potential risk of resulting in poorly defined or constantly evolving requirements [12]. This could lead to the development of software that does not fully meet the needs of users or satisfy operational demands. While continuous user engagement is intended to mitigate this risk, its effectiveness will depend on consistent and meaningful implementation. Traditional acquisition often involves extensive and detailed upfront requirements definition. The new pathways aim for more iterative refinement, but there is a possibility that initial requirements might be too vague or that user feedback may not be effectively incorporated, leading to rework or user dissatisfaction.

The rapid development and deployment of new software under Section 318 could present challenges in integrating with the Department of Defense's existing legacy systems, which are often complex and technologically outdated [6]. Issues related to interoperability between new and old systems could arise, potentially hindering the overall effectiveness of the deployed software. The DoD's current IT infrastructure comprises a vast array of legacy systems. Ensuring that new software developed under these pathways can seamlessly interact with these older systems will be a significant technical undertaking requiring careful planning and adherence to interoperability standards.

Despite the aim for increased efficiency, the utilization of new contracting mechanisms such as Other Transaction Authorities (OTAs) and Commercial Solutions Openings (CSOs), if not managed with appropriate diligence, could potentially lead to increased costs or a lack of accountability in the long term [2]. Ensuring proper oversight and robust contract management will be crucial to avoid these potential pitfalls. While OTAs and CSOs offer valuable flexibility and speed, their oversight and accountability mechanisms differ from those of traditional contracts. Therefore, responsible use of these tools and the development of expertise in their application are essential to ensure value for money and maintain adequate accountability.

Potential Negative Impact	**Proposed Mitigation**
Challenges in Adapting Existing Processes and Culture	Comprehensive training programs, communities of practice
Difficulty in Ensuring Cybersecurity in Rapid Development	Integrate security into every stage (DevSecOps), leverage enterprise services
Risk of Insufficient Requirements Definition	Mandate and facilitate continuous user engagement, iterative refinement
Challenges in Integrating with Legacy Systems	Develop integration guidelines and standards, prioritize interoperability, consider modular contracting
Potential for Increased Costs or Inefficiencies in the Long Run	Develop robust oversight mechanisms for OTAs and CSOs, ensure contracting officer expertise, emphasize performance-based outcomes

Mitigations the organization will take to diminish the negative impacts

To address the challenges associated with adapting to the new software acquisition pathways, the Department of Defense should implement comprehensive training programs for all relevant personnel. These programs should emphasize the core principles of Agile and DevSecOps methodologies and provide clear, practical guidance on the revised acquisition processes. Establishing communities of practice can further facilitate knowledge sharing and the development of best practices across different DoD components [5].

To mitigate the potential for compromised cybersecurity in the pursuit of rapid development, the DoD must integrate security requirements and testing into every stage of the software lifecycle. A strong emphasis should be placed on the "DevSecOps" approach, where security is a continuous and collaborative effort involving development, security, and operations teams [1]. Leveraging enterprise cybersecurity services can ensure that new software meets rigorous security standards without unduly slowing down the development process [1].

To counter the risk of poorly defined requirements, the Department should mandate and actively facilitate continuous engagement with software users throughout the entire development process. Clear channels for feedback must be established, and mechanisms put in place to ensure that user input is actively and effectively incorporated into the refinement of requirements and the iterative development cycles [12].

Addressing the challenges of integrating new software with existing legacy systems will require the development of clear guidelines and standards for software integration. The DoD should prioritize interoperability requirements in its acquisition strategies and invest in the necessary tools and expertise to facilitate seamless integration. Consideration should also be given to adopting modular contracting approaches and open system architectures to enhance the adaptability and integration capabilities of new software [17].

To prevent potential cost increases or inefficiencies associated with the use of OTAs and CSOs, the DoD must develop robust oversight mechanisms and contract management strategies specifically tailored for these alternative contracting methods. It is crucial to ensure that contracting officers receive the necessary training and develop the expertise required to effectively utilize these tools while maintaining accountability and ensuring responsible spending. Emphasizing performance-based outcomes in contracts can also help to ensure value for money [5].

DoD Personnel Most Affected

Program Managers will be at the forefront of implementing the new software acquisition pathways for their respective programs. They will need to adapt to the streamlined processes, fully embrace Agile methodologies, and ensure consistent and effective engagement with users throughout the software development lifecycle. A key aspect of their role will be understanding the implications of the provision that software acquired under these pathways will generally not be treated as a Major Defense Acquisition Program. This shift will likely require them to take on increased responsibility for rapid execution and adaptation, demanding a change in mindset and potentially the acquisition of new skill sets to effectively navigate this more flexible but also potentially more directly accountable environment.

Acquisition Officers and Contracting Officers will experience a significant shift in their responsibilities as they become proficient in utilizing alternative contracting mechanisms such as Commercial Solutions Openings (CSOs) and Other Transaction Authorities (OTAs) [1]. This will necessitate a move away from traditional Federal Acquisition Regulation (FAR)-based contracting procedures, requiring them to acquire new knowledge and skills in employing more flexible and commercially oriented acquisition methods. Their challenge will be to balance the need for speed and flexibility inherent in these new pathways with the critical responsibility of ensuring compliance with regulations and maintaining proper accountability for the expenditure of public funds.

Software Developers and Engineers, both within the government and among contractors, will need to adapt to working in more agile and iterative development environments. This will involve closer collaboration with users and a heightened focus on rapid prototyping and continuous integration and delivery of software capabilities [5]. Furthermore, they will bear a greater responsibility for prioritizing cybersecurity throughout the entire software development lifecycle [1]. This shift will demand adaptability and responsiveness to evolving requirements and a commitment to continuous improvement in their development practices.

Requirements Officers will see their role in defining and managing software requirements evolve significantly. They will need to shift their focus from creating detailed upfront specifications to articulating high-level needs and then prioritizing and iteratively refining those requirements based on ongoing user feedback [12]. A key aspect of this change is that software acquisition under these pathways will not be subject to the Joint Capabilities Integration and Development System Manual, which traditionally governs the requirements process for major acquisitions. This will require requirements officers to work more closely with users and developers throughout the software lifecycle, adopting a more dynamic and user-driven approach to defining and managing needs.

Cybersecurity Professionals will become even more integral to the software acquisition process, needing to be involved from the very beginning to ensure that security is "baked in" rather than added as an afterthought. They will need to collaborate closely with development teams to implement robust security measures and conduct continuous testing and evaluation throughout the software development lifecycle [1]. This proactive and collaborative approach to security will be essential to ensuring the cyber resilience of software acquired under these new pathways.

Stakeholders opposed and rationale for Opposition

Traditional Defense Contractors, accustomed to the often lengthy and highly detailed processes of traditional defense acquisition, may express opposition to the shift towards the faster, more flexible pathways outlined in Section 318. The increased emphasis on commercial solutions and the potential for greater involvement of non-traditional vendors could be perceived as a threat to their established business models and traditional revenue streams [1]. Their opposition may stem from concerns about potentially losing market share to smaller, more agile commercial companies, as well as anxieties regarding the reduced emphasis on detailed, long-term, large-scale contracts that have historically been their mainstay. They may also face internal challenges in adapting their established processes to the faster pace and iterative nature of the new software acquisition pathways.

Individuals within the Department of Defense Bureaucracy may also resist the changes introduced by Section 318. This resistance could be rooted in concerns about a perceived loss of control over acquisition processes, anxieties about reduced oversight despite the provision's intent for tailored oversight mechanisms, or simply a reluctance to learn and adopt new processes and methodologies. The explicit exemption of these software acquisition pathways from Department of Defense Directive 5000.01, a cornerstone of traditional defense acquisition, might be viewed by some within the bureaucracy as a reduction in necessary controls and rigor. Their opposition may arise from a comfort with established procedures and a potential skepticism towards the effectiveness and risks associated with the more streamlined pathways.

Advocates for Strict Regulatory Oversight, who prioritize meticulous adherence to established defense acquisition regulations and processes, may express concerns about the flexibility and potentially reduced documentation requirements under the new pathways. They might argue that deviating from traditional, well-established regulations could increase the risk of waste, fraud, and abuse, or lead to a failure to adequately address critical requirements and ensure proper accountability in the expenditure of taxpayer funds. Their opposition stems from a fundamental belief that the traditional regulations are essential for responsible stewardship and for mitigating the inherent risks associated with complex defense acquisitions.

Additional Resources

The successful implementation of Section 318's mandate for revised and codified software acquisition pathways will necessitate the allocation of several key additional resources to the Department of Defense.

Adequate Funding will be crucial to support the transition and ongoing operation of these new pathways. This includes investments in developing and delivering comprehensive training programs for DoD personnel, acquiring new tools and infrastructure required to support agile software development and DevSecOps practices, and potentially funding pilot programs to further refine the processes and address unforeseen challenges [6].

Comprehensive Training programs will be essential for ensuring that program managers, acquisition officers, contracting officers, software developers, and other relevant personnel fully understand and can effectively utilize the new software acquisition pathways. This training should cover the principles of Agile and DevSecOps methodologies, as well as the specific procedures for using Commercial Solutions Openings (CSOs) and Other Transaction Authorities (OTAs) [5].

The DoD may need to acquire Personnel with specialized expertise in modern software development methodologies, agile project management, cybersecurity, and commercial contracting to effectively implement and oversee these new pathways [17]. This could involve recruiting new personnel with these in-demand skills or investing in the retraining of existing staff to meet the evolving needs of the Department.

Investment in modern Software Tools and Infrastructure will be necessary to support the rapid development, continuous integration and delivery, and robust cybersecurity practices inherent in the new pathways. This may include the adoption of commercially available cloud computing platforms, the establishment of DevSecOps pipelines, and the deployment of collaborative development tools [1].

Finally, the development and dissemination of clear and comprehensive Guidance and

Best Practices will be critical to ensuring consistent and effective implementation of the new pathways across all relevant DoD components [5]. This should include the creation of standardized templates, the documentation of lessons learned from early adopters and pilot programs, and ongoing updates to reflect evolving best practices in software acquisition.

Measures of Success

The Department of Defense should employ a range of metrics to evaluate the success and effectiveness of the software acquisition pathways established under Section 318 once they are implemented.

A key measure will be the Time to Deployment, tracking the duration required to deliver new software capabilities to users under the new pathways compared to the timelines experienced with traditional acquisition methods. A significant and demonstrable reduction in deployment timelines will be a strong indicator of success [1].

Another important metric is the Frequency of Updates. The DoD should monitor how often software updates and new capabilities are delivered to ensure that the goal of at least annual updates, as mandated by Section 318(d)(3), is consistently being met and ideally exceeded.

User Satisfaction should be regularly assessed through feedback mechanisms to gauge how satisfied software users are with the delivered capabilities and the responsiveness of the development process [12]. Improvements in user satisfaction will signal that the new pathways are effectively meeting the needs of the warfighter.

The Adoption Rate of the new software acquisition pathways across different DoD programs should also be tracked. A high rate of adoption would suggest that program managers and acquisition professionals perceive the new pathways as valuable and effective tools for acquiring software.

Cybersecurity Metrics will be crucial for evaluating the security posture of software developed under these pathways. This includes tracking the number of vulnerabilities identified and resolved, the time taken to address security issues, and the overall security posture of the deployed software [1].

Analyzing the Cost Efficiency of acquiring software under the new pathways compared to traditional methods will be important for demonstrating responsible use of taxpayer funds. The DoD should look for evidence of potential cost savings or improved value for money.

Finally, the extent to which the new pathways facilitate Innovation Adoption should be measured. This includes tracking the involvement of non-traditional vendors and the adoption of cutting-edge commercial technologies in DoD software acquisitions [1].

Alternative approaches

While Section 318 mandates the establishment of specific software acquisition pathways, alternative approaches could have been considered to achieve similar outcomes of faster and more efficient software delivery within the Department of Defense.

One alternative could have been an Incremental Reform of Existing Processes. Instead of codifying entirely new pathways, the DoD might have focused on gradually reforming traditional acquisition processes to incorporate more agile principles and shorter timelines. This approach might have been less disruptive to the existing acquisition bureaucracy but potentially less transformative in its impact.

Another option could have been a primary Focus on Policy and Guidance Updates. The DoD could have relied solely on updating existing policies and guidance documents, such as DOD Instruction 5000.87, to strongly encourage the adoption of agile and rapid software acquisition methodologies, without seeking legislative codification. However, this approach might have lacked the permanence and authoritative weight of law.

A more cautious approach could have involved extensive Pilot Programs and Best Practice Sharing across various DoD components. This would have allowed for the identification of effective strategies and lessons learned for rapid software acquisition before codifying specific pathways into law. While potentially reducing the risk of unintended consequences, this approach might have resulted in a longer timeframe for achieving widespread reform.

Finally, an alternative or complementary approach could have placed a greater Emphasis on Training and Cultural Change within the acquisition workforce. Focusing primarily on educating personnel in modern software development practices and fostering a culture of agility and innovation might have been pursued. While crucial for the success of any new acquisition approach, this alone might not have been sufficient to overcome deeply entrenched systemic and bureaucratic hurdles.

Section Specific Question 1: How does Section 318 formally codify or modify the

specific DoD pathways for software acquisition (e.g., Agile, DevSecOps)? What are the core tenets or requirements Program Managers must follow when using these pathways?

Section 318 formally codifies the establishment of software acquisition pathways within the Department of Defense by adding a new section, 3603, to Title 10 of the United States Code [4]. Specifically, it mandates the Secretary of Defense to establish pathways for the efficient and effective acquisition, development, integration, and timely delivery of software and covered hardware. The provision explicitly requires the establishment of at least two pathways: one for applications and another for embedded systems. While Section 318 does not explicitly mandate the use of terms like "Agile" or "DevSecOps," it strongly promotes their underlying principles. It emphasizes rapid development and implementation, the use of proven technologies and solutions to continuously engineer and deliver capabilities, the initiation of new software capabilities quickly with demonstration of viability within one year, and the continuous updating and delivery of new capabilities at least annually. Furthermore, Section 318(h) requires the Secretary to tailor streamlined policies and processes relating to iteratively developing, integrating, testing, and fielding capability, as well as ensuring the delivery of cyber secure systems, all of which align with the principles of Agile and DevSecOps [5]. A significant modification to existing processes is the explicit exemption of software acquisition under these pathways from the Joint Capabilities Integration and Development System Manual and Department of Defense Directive 5000.01, which are central to traditional defense acquisition. The repeal of Section 800 of the FY2020 NDAA further underscores the intent to establish a new, codified framework for software acquisition.

Program Managers utilizing these pathways must adhere to several core tenets and requirements. They must prioritize the use of proven technologies and solutions to ensure efficient and effective delivery. A critical requirement is to demonstrate the viability and effectiveness of new software capabilities for operational use within one year after funds are first obligated. Program Managers are also responsible for ensuring the continuous updating and delivery of new capabilities at least annually to iteratively meet user needs. They must adopt a risk-based approach when considering innovative technologies and follow a streamlined and coordinated requirements, budget, and acquisition process to support rapid fielding within a year. Continuous engagement with the users of the software is mandatory to support both engineering activities and the delivery of software for operational use. Furthermore, Program Managers must tailor streamlined policies and processes related to various acquisition elements, including user needs, prioritization, user engagement, acquisition strategies, awarding contracts, iteratively developing, integrating, testing, and fielding capability, and crucially, ensuring the delivery of cyber secure systems.

Section Specific Question 2: (This question is currently empty and will be addressed if further information is provided.)

Summary

Section 318 of the FoRGED Act represents a fundamental shift in the Department of Defense's approach to software acquisition. By establishing and codifying specific pathways, the provision aims to overcome the limitations of traditional acquisition processes and enable the faster, more efficient, and more agile delivery of software capabilities to the warfighter. The emphasis on speed, continuous improvement, user engagement, and cybersecurity reflects a recognition of the critical role software plays in modern defense. While the potential benefits of this reform are significant, the successful implementation of Section 318 will require a concerted effort to address potential challenges, provide the necessary resources, and foster a cultural transformation within the DoD acquisition community. Ultimately, the effectiveness of this provision will be judged by its ability to accelerate the delivery of secure and effective software solutions that enhance the lethality and operational capabilities of the United States military.

Works cited

1. Modern Software Acquisition to Speed Delivery, Boost Warfighter Lethality, accessed March 30, 2025, https://www.defense.gov/News/News-Stories/Article/Article/4114775/modern-software-acquisition-to-speed-delivery-boost-warfighter-lethality/
2. Hegseth issues edict on DOD software acquisition - DefenseScoop, accessed March 30, 2025, https://defensescoop.com/2025/03/07/hegseth-memo-dod-software-acquisition-pathway-cso-ota/
3. MAR - 6 2025 - Department of Defense, accessed March 30, 2025, https://media.defense.gov/2025/Mar/07/2003662943/-1/-1/1/DIRECTING-MODERN-SOFTWARE-ACQUISITION-TO-MAXIMIZE-LETHALITY.PDF
4. Text - S.5618 - 118th Congress (2023-2024): FoRGED Act, accessed March 30, 2025, https://www.congress.gov/bill/118th-congress/senate-bill/5618/text
5. DOD Mandates Use of Software Acquisition Pathway for Software Development Procurements - Wiley Rein, accessed March 30, 2025, https://www.wiley.law/alert-DOD-Mandates-Use-of-Software-Acquisition-Pathway-for-Software-Development-Procurements
6. Hegseth signs memo pushing forward Software Acquisition Pathway expansion, accessed March 30, 2025,

http://breakingdefense.com/2025/03/hegseth-signs-memo-pushing-forward-software-acquisition-pathway-expansion/

7. DoD Reaffirms Software Acquisition Pathway Use - AFCEA International, accessed March 30, 2025, https://www.afcea.org/signal-media/defense-operations/dod-reaffirms-software-acquisition-pathway-use
8. Software Acquisition Pathway (SWP) | www.dau.edu, accessed March 30, 2025, https://www.dau.edu/aafdid/swa
9. Text - S.5618 - 118th Congress (2023-2024): FoRGED Act ..., accessed March 30, 2025, https://www.congress.gov/bill/118th-congress/senate-bill/5618/text/is?format=txt
10. Advancing DoD Operations With Software Acquisition Reform - Defense Innovation Unit, accessed March 30, 2025, https://www.diu.mil/latest/advancing-dod-operational-capabilities-with-software-acquisition-reform
11. DOD Looking to Reform Software Acquisition - HS Today, accessed March 30, 2025, https://www.hstoday.us/dod-national-defense/dod-looking-to-reform-software-acquisition/
12. Evolving DOD Software Acquisition - DAU, accessed March 30, 2025, https://www.dau.edu/sites/default/files/2024-01/GAO%20%20Software%20Acquisition%20Slides%20FINAL.pdf
13. DOD Acquisition Reform: Military Departments Should Take Steps to Facilitate Speed and Innovation - Government Accountability Office (GAO), accessed March 30, 2025, https://www.gao.gov/products/gao-25-107003
14. GAO: DoD Needs to Embrace Iterative Development for Acquisitions - MeriTalk, accessed March 30, 2025, https://www.meritalk.com/articles/gao-dod-needs-to-embrace-iterative-development-for-acquisitions/
15. Finally–DoD Software Acquisition Reform - Knowmadics, accessed March 30, 2025, https://knowmadics.com/dod-software-acquisition-reform/
16. Two vastly different Army programs prepare for Software Acquisition Pathway, accessed March 30, 2025, https://www.eis.army.mil/newsroom/news/peo-enterprise-wide/two-vastly-different-army-programs-prepare-software-acquisition
17. The Software Advantage - Line of Departure - Army.mil, accessed March 30, 2025, https://www.lineofdeparture.army.mil/Journals/Army-AL-T/Spring-2024/The-Software-Advantage/
18. Overcoming 4 Software Development Challenges within the DOD | Galvanize, accessed March 30, 2025, https://www.galvanize.com/blog/overcoming-4-software-development-challenges-within-the-dod/