Software Assurance Tips

A product of the Software Assurance Tips Team[5]

Jon Hood

Monday 26th January, 2026

1 Unsafe at Any Speed: The Designed-In Dangers of DevSecOps

Updated Tuesday 27th January, 2026

1.1 Introduction

In 1965, Ralph Nader published his book, *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile.* In it, one of his critiques included the ignorance of "Crashworthiness" standards, claiming that vehicle manufacturers knew about the secondary crash events (riders hitting the internal parts of a vehicle and suffering injury) but chose to save cost and do nothing about it.

Sixty years later, we have an administration pushing forward sound standards that are actively being ignored and redefined. In this week's SwATip, we'll take a look at the Department of War's latest software development memorandums and guidelines, then get a boots-on-the-ground look at how they're being redefined.

Lethal Speed

In March 2025, Secretary Hegseth published a memo directing the Department of Defense to adopt the Software Acquisition Pathway (SWP), DoDI 5000.87, as the means of acquiring, developing, and iterating updates for software.[2]

The false claim is that the DoD/DoW is focusing on fielding quickly in favor of lethality rather than bureaucratic processes like software assurance, validation, and accreditation. Software development organizations are pointing to this memo as justification for completely skipping the processes that make code delivery secure.

Reality is the exact opposite. Instead, SWP pushes the old DoD way of doing things into the modern era. "Cybersecurity and program protection will be addressed from program inception throughout the program's lifecycle…" Instead of a point-in-time inspection and waterfall-like process of evaluating software after it's written, cybersecurity policies related to software must perform the cybersecurity validation as part of the development process, earlier in the lifecycle when it will not slow down deployment. "Software assurance, cyber security, test and evaluation are integral parts of this approach to continually assess and measure cybersecurity preparedness and responsiveness, identify and address risks and execute mitigation actions."[1] Leadership is forcing something that we've seen for decades: the need to bring cybersecurity assessment into the development pipelines early.[4]

The DoW isn't saying to just ignore the processes that identify risks. Yes, the need to field and achieve lethality may be greater than the risk of fielding, but that risk should still be enumerated and identified as early in the process as possible.

RMF Is Dead

In September 2025, the DoW announced the move to the Cybersecurity Risk Management Construct (CSRMC). The Risk Management Framework's (RMF) documentation-heavy approach relied on static point-in-time inspections and checklists, a concept already denounced in the aforementioned Hegseth memo.

The partially false claim is that RMF is dead; therefore, its cybersecurity requirements are no longer valid.

Reality is that cybersecurity professionals engaged in technical activities are celebrating. CSRMC moves from these static assessments to the continuous assessment frameworks already accounted for in the RMF continuous monitoring construct. This frees up cybersecurity teams. Instead of point-in-time inspections, they must rely on automated, AI-enabled tools to continuously assess networks, systems, and components. The standard is no longer whether a cybersecurity professional can spend weeks or even months documenting their findings and getting security managers to push their assessment results into eMASS; it's now on their ability to flag concerns in the automated and continuous assessment pipelines that are now required. Red teaming, blue teaming, and pentesting are all moved into the **Test** portion of the CSRMC while Software Assurance is embedded into the security requirements of the architecture in the very first **Design** phase.

The reports of RMF's death are greatly exaggerated. Had your program been implementing continuous monitoring, "RMF 2.0," or continuous ATO guidance, it would be in shape to implement what's coming with CSRMC. Shifting left into automated pipelines instead of documenting findings in reports attached to eMASS that are ignored until there's a problem represents a proactive (rather than reactive) cybersecurity posture.

Less Cybersecurity Training

Also in September, Secretary Hegseth announced a reduction in mandatory annual training.[6] In the memo, Secretary Hegseth instructed the CIO to relax the mandatory frequency for cybersecurity training.[3]

The false claim is that cybersecurity training and requirements are being eliminated.

Reality is that consolidating and simplifying the frequency of addressing these topics helps prioritize the execution of warfighting, strengthening lethality (tying it to the first memorandum).

Biden-Era Software Assurance Is Rescinded

In January 2026, the Office of Management and Budget published a memo rescinding the Biden-era SBOM requirements, moving the monolithic SBOM approach decisions back to the project offices to implement supply chain security as they deem appropriate for their programs.[7]

The false claim has been made that broadly applies this rescission to all of Software Assurance when the focus is on dependency lists, Bills of Material, and other supply chain security requirements.

Reality is that the burden of software security is not one-size-fits-all. Giving the programs back their authority to determine software security puts risk decisions back into the management chain where it belongs. "Agencies shall continue to maintain a complete inventory of software and hardware and develop software and hardware assurance policies and processes that match their risk determinations and mission needs."

Conclusion

Another critique in Nader's *Unsafe at Any Speed* is that those responsible for developing vehicles would blame "the nut behind the wheel," shifting safety and operation to the driver's fault rather than building a sound vehicle that could protect them better. Today, we are seeing outrage at sound policies that can be implemented appropriately and safely. Nevertheless, there has been no shortage of development organizations attempting to convince leadership to ignore cybersecurity in favor of going fast. These organizations abuse the memorandums and standards established for them and

construct a fortress around themselves to protect them from the fallout. DevSecOps environments are created on the platforms which shift risk and blame to external stakeholders who cannot mitigate it rather than taking the accountability demanded by leadership.

Nader ended his book noting the coming struggle for safety, begging the government to step in and reform the organizations that prioritized profits over safety. Today we stand on the edge of that happening again: can vendors be trusted to police themselves by bringing the cybersecurity responsibilities into the development pipeline, or will they commit the same mistakes as the auto industry of the 1960's by relaxing cybersecurity standards and blaming others? If you hear of a development organization pushing any of the false claims documented here, then it may be already too late. The development organization isn't "shifting left" and moving cybersecurity where it is mandated to be; they're simply doing nothing and hoping for the best.

References

[1] Department of Defense. Department of Defense Instruction 5000.87. Operation of the Software Acquisition Pat Tech. rep. Washington, D.C.: Department of Defense, 2020. URL: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF.

[2] Peter Hegseth. Directing Modern Software Acquisition to Maximize Lethality. 2025. URL: https://media.defense.gov/2025/Mar/07/2003662943/-1/-1/1/DIRECTING-MODERN-SOFTWARE-ACQUISITION-TO-MAXIMIZE-LETHALITY.PDF.

[3] Peter Hegseth. Reduction of Mandatory Training Requirements to Restore Mission Focus. 2025. URL: https://media.defense.gov/2025/Sep/30/2003812317/-1/-1/1/SECRETARY-OF-WAR-ANNOUNCED-MEMORANDUMS.PDF.

[4] Jon Hood. "Defensive Development Plans". In: SwATips.com (2025). URL: https://www.swatips.com/articles/20250127.html.

[5] Jon Hood, ed. SwATips. https://www.SwATips.com/.

[6] U.S. Department of War. "Hegseth Announces War Department Reforms in Sweeping Speech to Top Military Brass". In: (Sept. 2025). URL: https://www.war.gov/News/News-Stories/Article/Article/4318394/hegseth-announces-war-department-reforms-in-sweeping-speech-to-top-military-bra/.

[7] Russell Vought. Adopting a Risk-based Approach to Software and Hardware Security. 2026. URL: https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf.