SYM-AM-25-421

Excerpt from the Proceedings

of the

Twenty-Second Annual Acquisition Research Symposium and Innovation Summit

Volume III

An Assurance Educated Workforce Is Critical to Addressing Software and Supply Chain Acquisition Lifecycle Risks

Published: May 5, 2025

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

An Assurance Educated Workforce Is Critical to Addressing Software and Supply Chain Acquisition Lifecycle Risks

Dr. Carol Woody—is a Principal Researcher for the CERT division of the Software Engineering Institute at Carnegie Mellon University. She leads a team that builds capabilities and competencies for measuring, managing, and sustaining software assurance and cybersecurity for highly complex software-intensive systems and supply chains throughout the acquisition lifecycle. She coauthored a book, Cyber Security Engineering: A Practical Approach for Systems and Software Assurance, published by Pearson Education as part of the SEI Series in Software Engineering. The CERT Cybersecurity Engineering and Software Assurance Professional Certificate is based on the research she led. [cwoody@cedrt.org]

Abstract

Today's systems are software-intensive and complex, with a growing reliance on third-party technology. Through reuse, systems can be assembled faster with less development cost. Traditionally, systems were hardware-based, and operational risks were primarily linked to reliability. Now systems are largely software-based, which does not wear out like hardware, and the critical risks are different. All software contains vulnerabilities that are hard enough to manage directly. Inheritance through the supply chain increases the management challenges and magnifies the risk of a potential compromise. Attacks on the software supply chain are increasingly frequent and devastating. Software risk management capabilities are brought in too late, if at all, to identify and address software risks that can appear throughout the lifecycle. Extensive compliance rules have been put in place for federal acquisitions to address software and supply chain risk, but there is a noticeable gap in the current acquisition and engineering workforce's knowledge and skills needed to address the rules effectively. Expanding the knowledge of decision-makers and participants in system acquisition, engineering, and integration are critical activities that are necessary to address the growing software risk.

Introduction

Today's systems are increasingly software-intensive and complex, with a growing reliance on third-party technology. Through reuse, systems can be assembled faster with less development cost. Traditionally, systems were hardware-based, and operational risks were primarily linked to reliability. Now systems are largely software-based, which does not wear out like hardware, and the critical risks are different. All software contains vulnerabilities that are hard enough to manage directly. Inheritance through the supply chain increases the management challenges and magnifies the risk of a potential compromise. In addition, suppliers can become propagators of malware and ransomware through features that provide automatic updates. Attacks on the software supply chain are increasingly frequent and devastating.

Extensive compliance rules have been put in place for federal acquisitions to address software and supply chain risk, but there is a noticeable gap in the current acquisition and engineering workforce's knowledge and skills needed to address the rules effectively. Each program develops their unique risk management processes and practices, many of which ignore software. The right capabilities are brought in too late, if at all, to identify and address software risks that can appear throughout the lifecycle. Acquisition and program management are focused on budgets, cost, and schedule, motivating the adoption of shortcuts even in addressing compliance. Expanding the knowledge of decision-makers and participants in system acquisition and engineering is a critical component in addressing the growing software risk, but it does not appear to be anyone's responsibility.

In his memo from March 6, 2025, on *Directing Modern Software Acquisition to Maximize Lethality*, the Secretary of Defense (2025) noted the following:

> The Department of Defense (DoD) has been slow to recognize that software-defined warfare is not a future construct, but the reality we find ourselves operating in today. Software is at the core of every weapon and supporting system we field to remain the strongest, most lethal fighting force in the world. While the commercial industry has rapidly adjusted to a software-defined product reality, DoD has struggled to reframe our acquisition process from a hardware-centric to a software-centric approach.

Unfortunately, recent experience at Carnegie Mellon University Software Engineering Institute (CMU SEI) for weapon and support systems has shown that directing the resources that have efficiently handled the DoD acquisition process for decades to now focus on software will not be sufficient. Software is designed, built, integrated, managed, and supported differently from hardware. Current processes and practices have not been tailored and integrated for effectively addressing these differences. Software is also not isolated to specific segments of the system but has become a major portion of virtually all aspects of system development and delivery, requiring an integrated perspective for effective management.

The various participants in an acquisition program focus on their existing areas with expertise limited to their current functions and are only tied to other areas by processes that share data, documents, or dollars to efficiently deliver capabilities as they continue functioning under a hardware-oriented approach. Figure 1 provides a high-level view into the structure of a major acquisition.

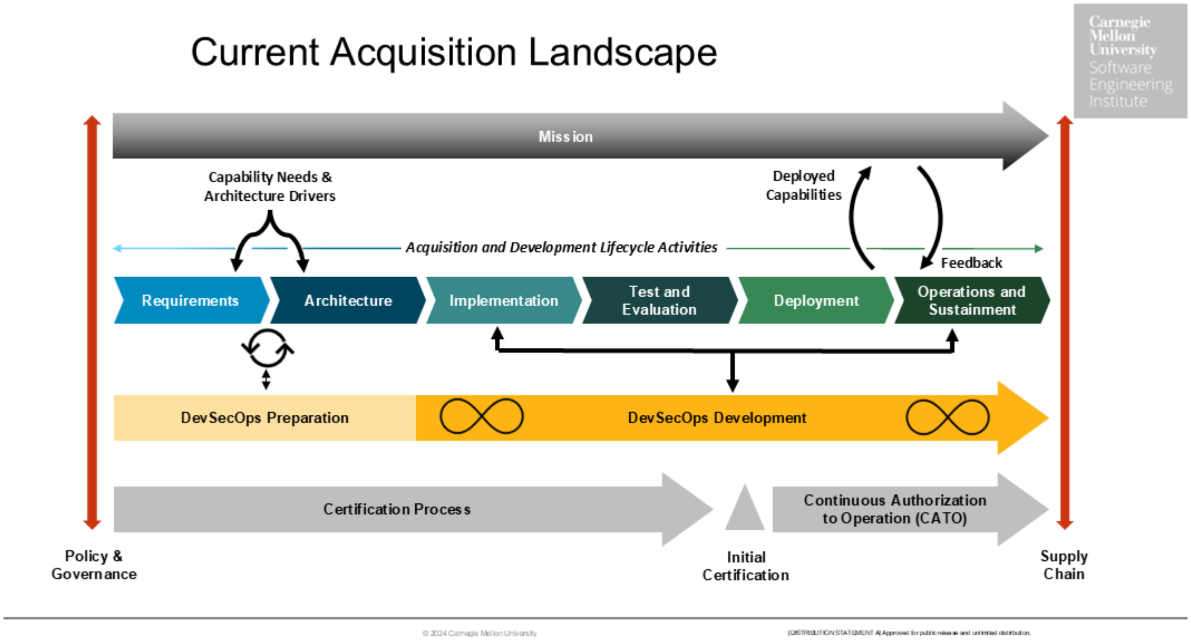
Current Acquisition Landscape
Carnegie Mellon University Software Engineering Institute
Mission
Capability Needs & Architecture Drivers
Deployed Capabilities
Acquisition and Development Lifecycle Activities
Feedback
Requirements
Architecture
Implementation
Test and Evaluation
Deployment
Operations and Sustainment
DevSecOps Preparation
DevSecOps Development
Certification Process
Continuous Authorization to Operation (CATO)
Policy & Governance
Initial Certification
Supply Chain
© 2024 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Figure 1. Current Acquisition Landscape

The program management for a major DoD acquisition focuses on the mission and the warfighter capabilities needed to expand mission capabilities (top line in Figure 1). Their primary acquisition product is the statement of work (SOW), which lays out the range of requirements that a contractor will be asked to deliver (including mandatory policy guidance drawn from the line up the left of Figure 1 and compliance drawn from the bottom line in Figure 1). From the SOW, system engineers working for the government (addressing the acquisition and development lifecycle activities in Figure 1) will develop a system specification and system engineering plan (SEP) as part of the activities in the second layer of the acquisition to decompose the SOW with further detail about the engineering rigor expected from the vendor. In parallel, cybersecurity experts (bottom line on Figure 1) are creating a program protection plan (PPP), which is expected to contain a cybersecurity strategy (CSS) defining the requirements for security controls on the system. Engineers from the contractor will use the SOW, SEP, and PPP to build a software development plan (SDP). From the SDP, the contractor—and government, if the final product will be owned by the government—will assemble the tools in development pipelines to automate, as feasible, the software production process (DevSecOps line in Figure 1). There may be many development pipelines addressing various classification levels of the system and software. Software is frequently missing from early milestones, and feedback loops from cybersecurity monitoring and software development to program cost and schedule typically do not exist. These challenges can lead to risk and cost impacts that continue into operations where they are much more costly to address.

At various milestone reviews sprinkled within the acquisition schedule, participants evaluate progress through various processes that involve the review of documents delivered by the contractor. These interactions involve many steps, multiple organizational entities, suppliers, and document exchanges. Eventually they can result in a poorly managed project plan with uncertain cost and schedule milestones. Lacking the knowledge and required integration across government teams necessary to effectively deliver a system in the software-intensive environments we face today, the system can be plagued by inconsistent processes, disjointed compliance-driven risk management plans, and cost-schedule overruns. A more troubling outcome can be a variety of separate views that do not ensure agreement as to what is delivered.

DoD Instruction 5000.02 (Office of the Under Secretary of Defense for Acquisition and Sustainment, 2020) establishes the management framework for translating mission needs and technology opportunities, based on approved mission needs and requirements, into stable, affordable, and well-managed acquisition programs that include weapon systems and automated information systems (AISs):

> To achieve those objectives, Milestone Decision Authorities (MDAs), other Decision Authorities (DAs), and Program Managers (PMs) have broad authority to plan and manage their programs consistent with sound business practice. The AAF acquisition pathways provide opportunities for MDAs/DAs and PMs to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired. (Office of the Under Secretary of Defense for Acquisition and Sustainment, 2020, p. 4)

Both software and its assurance are latecomers to the acquisition lifecycle. As shown in Figure 1, software's role has been assigned primarily to the bottom two layers of the structure: the pipeline where it is built and the certification process. Unfortunately, many decisions that impact software are made early in the acquisition by system engineers, contracting, and supply chain management that directly impact the assurance of the software, but those with software expertise are typically not included in these earlier steps.

Systems engineers have dominated the early stages of the acquisition and development lifecycle in both the government and defense contractor organizations following the Department of Defense Architecture Framework (DoDAF) principles (DoD Chief Information Officer, 2010), creating elaborate overview and detail diagrams that show how a new system will be interfaced with existing capabilities and built from components. Software has long been relegated to the lower tiers of the DoDAF. Systems engineers decompose the capabilities into independent components, following good engineering practice (INCOSE, 2023) to reduce the complexity needed to be considered as each individual component is built. The assembly of the components is expected to yield the desired capabilities with the desired qualities (such as security and safety), which are emergent properties of the integrated whole. Each component is assigned functional requirements that flow down from the SOW and SEP. Interfaces among components are assumed to be well formed and isolated. Risks are evaluated at the system level, and appropriate controls are incorporated into the design to ensure the requirements for security based on confidentiality, integrity, and availability are met, and these will be evaluated for compliance by cybersecurity experts before the system will receive an authority to operate (bottom line in Figure 1). Too frequently, the processes are not well managed and integrated by individuals with the skills necessary to ensure that software considerations are addressed appropriately.

As part of the modernization planning, the DoD is migrating storage usage to cloud services and outsourcing other capabilities to reduce infrastructure costs and enhance enterprise capabilities to share information (DoD Chief Information Officer, 2024). These services are primarily software-based, further increasing the layers of software incorporated into an acquisition. These choices are typically made by program management and shift the control of this software from system engineering to supply chain management, but software expertise is not typically part of this team. The third-party software components may include additional capabilities that expand the available functionality and external interfaces and violate the independence of the components.

The DoD is also embracing modernization of software development using Agile techniques for incremental development and software factories. Tools for the factory pipelines may augment the code such that the functionality delivered goes beyond the original requirements, which can violate isolation assumptions and result in the inclusion of capabilities that allow bypassing of security controls implemented at the system level. Unless the system engineers prepare the system design to be implemented incrementally, the software factory selection of what will be done and in what order will be made at the software development stages. Choices for the sequence of what portions are developed may determine the readiness of the system for meeting the system's qualities (such as security and safety) and conflict with program management expectations for implementation.

When software is created, available modules and code libraries from third parties that provide the functionality needed are extensively reused, creating an unexpected dependency on the supply chain. Management and oversight of those suppliers is frequently overlooked due to lack of software expertise and skills. Software components are often interrelated sets of functionality (one layer is *not* necessarily contained inside another layer), and routines that address shared functionality are created as shared subroutines interfaced to multiple modules instead of repeated inside each of the use points. This minimizes the maintenance requirements of the code in the future since all uses are taken from one source but violates the independent assumptions of each individual software component inherent in the system design.

Gaps in Program Knowledge About Software Risks

As noted earlier, software is designed, developed, managed, and monitored uniquely. Software is intellectual property and is the output of creativity and knowledge of its writer. A reality with software is that all software contains potential vulnerabilities: either inserted through gaps in the language structures if secure coding standards are not enforced or inherited from reused components—or both. For many third-party software products and open-source products, these vulnerabilities are publicly available through the National Vulnerability Database (National Institute of Standards and Technology [NIST], n.d.). Too frequently, there is a lack of recognition of the risks these vulnerabilities represent to the program. The PPP should include considerations for software risks, but software expertise is typically missing in the supply chain risk management teams that have responsibility for this document. Cybersecurity may be enforcing the NIST Risk Management Framework (RMF; NIST, 2018), which includes recommendations for vulnerability identification through the application of static and dynamic analysis tools. However, to reduce the vulnerability risk to a program, the requirements for the acquisition must include removal of these vulnerabilities; this removal must be incorporated into either the pipeline activities for the software factory or managed through the input to the pipeline as a backlog entry. Handling of vulnerabilities in third-party software, which a program does not directly control, may require software design constraints. These constraints need to be managed in a program software architecture, which is too frequently disbursed into each software component as part of the system architecture without consideration of system-wide needs that should be integrated across the program.

Software products cannot be implemented and ignored. Few programs recognize the realities of software reliability that must be constantly monitored for obsolescence, changes in business needs that require adjustments, and new vulnerabilities discovered by others and published, increasing the risk to those still using the software. Even if the risks are identified and reported, risk management procedures are too frequently not integrated with software management activities. At the SEI, we see many organizations in which software risks are reported and collected when software is being developed, but the organizations lack mechanisms for escalating these risks to program decision-makers. Lacking an awareness of the software risks, program leaders do not know when and how to respond until a crisis occurs.

Program management monitors the cost and schedule for the acquisition and is focused on effective delivery of the requirements as defined in the SOW. Too frequently, the development of the SOW does not integrate cybersecurity, software assurance, and software supply chain risk management requirements. Even when these requirements are included, personnel knowledgeable in software and cybersecurity are typically not part of the early lifecycle activities; therefore, consideration in the early planning and engineering is missed. Too frequently, the SOW will require meeting such specific policies as AFMAN 91-119 (DefenseMirror.com, 2024) and NIST 800-53 (NIST, 2018) and require the contractor to address the RMF as the cybersecurity requirements. These policies and standards are written at a general guidance level that must be tailored to specific risk considerations for the program; however, without the proper expertise, appropriate tailoring is not happening. The contractor may select controls that are insufficient for the actual risks without providing clarity as to the specific software and cybersecurity concerns to be addressed, driven by a compliance mentality, without adequate tailoring to address the software-related risks. In other instances, only external system risks that are mandated for compliance are considered, and software risks that are based on supply chain decisions (made by both the prime contractor in handling their subcontractors and the government in their software supply chain) are overlooked.

Program Needs for Risk Management of Software

Having the right knowledge to recognize and understand cybersecurity and software risks throughout the acquisition and development lifecycle is critical. Program management, systems engineers, and supply chain acquisition resources need to understand the risks to the program/system and appropriately identify and manage them throughout the lifecycle. This knowledge is not currently part of the expertise required for these positions. Having an effective risk management framework in place to connect software risks with the handling of program risks is critical to the success for programs with intensive software and software supply chain components.

Program leadership and acquisition personnel need to know how to address the following issues: (1) When do we need to include software, cybersecurity, and software supply chain expertise? (2) How do we get the resources we need at the right place in the program to address the growing needs for software and supply chain risk management (SCRM) with a workforce that is currently not prepared to handle these responsibilities and a pipeline of future workers who have never heard about software vulnerabilities in their education, much less learned how to address them? In addition, program leadership must understand that responsibility for software is widely scattered across all parts of the acquisition and development lifecycle, and collaboration among these various players is typically nonexistent. The ability to build and manage the processes that are required for software-intensive systems is essential and requires that software informed expertise and training become a priority.

Different program groups develop the SOW, SEP, and PPP. When software and cybersecurity are included, they need to be consistent and integrated, and in most cases, we have seen wide discrepancies among the requirements in each of these documents. At a minimum, we must raise the awareness of leadership that software-intensive systems require new skills, training, and an expanded management mindset. Today's acquisitions are increasingly software-intensive, complex, and reliant on third-party technology (i.e., hardware, software, and firmware).

The strategic transition to commercial software can serve to expand software risk management to a more lifecycle-oriented perspective. Programs will rely more on vendors that address security issues through patches and upgrades that must be constantly monitored and integrated. As vendors release new versions, older products are no longer maintained, and existing vulnerabilities are not addressed. Programs are not currently structured to continuously update third-party and open source software products. Obsolescence will be a growing issue for an environment that is accustomed to long implementation cycles. The DoD leadership guidelines do not come with consideration of the shift in responsibilities to address the expanded role that software-intensive systems bring. Risk decisions made by acquisition personnel must expand beyond the lowest cost and include strategies that address the increased risk posed in a software-intensive environment.

Framework for Effective Software Risk Management

Personnel to address software assurance need to be integrated into every acquisition from the start. These individuals need to understand how systems can be compromised by software; they also need to be aware of mechanisms available for software risk mitigation and how to connect the opportunities for effective management of software concerns into the range of acquisition activities underway at the program and system level

The responsibility for software assurance is laid out by the DoD as follows (DoD Chief Information Officer, 2024):

> *Software Assurance:* The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

In establishing confidence that the system will be delivered with appropriate software assurance, those addressing software must assemble information from the contractor, government oversight, and across the program early in the lifecycle to predict the level of software assurance that is required based on available evidence and course correct as needed throughout the lifecycle. Later in the lifecycle, software assurance personnel will need to collect data to confirm that results are as expected; this validation will be done in preparation for final verification prior to planned deployment and transition into sustainment activities for monitoring and management of software risk.

SEI researchers, led by the author, have been working with major federal programs to identify effective processes and practices for software assurance and supply chain risk management and have published them in the Acquisition Security Framework (ASF; Alberts et al., 2022). In addition, we conducted two panels at the Software and Supply Chain Assurance Forum: the first in January 2024 on “Establishing the Demand Signal for Good Software Assurance” and the second in May 2024 on “Positioning for Software Assurance Success: Practices, Tools & Technology, Knowledge & Skills.” The programs supporting these panel discussions have experience in addressing the challenges of software assurance and software supply chain risk. All of them identify education of program leadership and acquisition integration as primary considerations for success.

It is critical to ensure that the expertise needed is in the right place, and the understanding of the criticality of having this expertise falls on program management. Programs can acquire these capabilities or grow them. In addition, the DoD should consider how to more effectively provide this level of expertise for program use. The Defense Acquisition University (n.d.) is assembling training to support this critical need, but current expertise is limited. There are challenging questions to be addressed by each program:

- Who do we hire or educate?
- What do they need to know to address software and supply chain risk for a program’s areas of responsibility?
- How should they learn about what they need to know?
- What expanded collaborations are needed within the lifecycle for the program to provide effective operational results?
- Who is available to the program leadership currently showing success in handling software and supply chain risk to share lessons learned?

Future Considerations

Software vulnerability risk and software supply chain risk are major attack vectors for all technology, and the growth rate is exponential. However, DoD programs appear to not recognize this sufficiently early in the acquisition lifecycle to plan for cost-effective mitigations; instead, consideration is deferred into system integration stages when correcting the gaps is very costly. Because software risk is not well understood by the programs as a key responsibility, DoD funding for specified actions to address software issues is driving the level of consideration provided. As an example, recent mandates to create software bill of materials (SBOMs; Executive Office of the President of the United States, 2022) support improving software supply chain visibility, but programs are claiming this is an unfunded mandate that they are not funded to address. The gaps in understanding software risk and the imperatives for cost-effective execution require an assurance-educated leadership to provide appropriate guidance and an assurance-educated workforce to know how to effectively address the challenges.

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References

Alberts, C., Bandor, M., Wallen, C., & Woody, C. (2022, October 31). Acquisition security framework (ASF): Managing systems cybersecurity risk. *Carnegie Mellon University Software Engineering Institute*. https://doi.org/10.1184/R1/21357627

Defense Acquisition University. (n.d.). *Software acquisition - software acquisition (SWA) resources.* Retrieved April 25, 2025, from https://www.dau.edu/aaf/swa/resources

Defensemirror.com bureau. (2024, May 10). *DoD Inspector General’s office evaluates U.S.A.F.’s nuclear design certification for aircraft carrying B61-12 nuclear bomb.* https://www.defensemirror.com/news/36762

DoD Chief Information Officer. (2010, August). *The DoDAF architecture framework version 2.02.* https://dodcio.defense.gov/Library/DoD-Architecture-Framework/

DoD Chief Information Officer. (2024, September 24). *Memorandum for senior pentagon leadership defense agency and DOD field activity directors: Department of Defense cloud financial operations strategy*. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDCloudFinOpsStrategy.pdf

Executive Office of the President of the United States. (2022, September 14). *Memorandum for the heads of executive departments and agencies: Enhancing the security of the software supply chain through secure software development practices* (Report No. OMB M-22-18). https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

INCOSE. (2023). *Systems engineering handbook: A guide for system life cycle processes and activities, version 5.0*. John Wiley and Sons, Inc.

National Institute of Standards and Technology. (n.d.). *National vulnerability database (NVD)* (SP 800-52 Rev 2). Department of Commerce. https://nvd.nist.gov/

National Institute of Standards and Technology. (2018, December). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (SP 800-37 Rev. 2). Department of Commerce. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Office of the Under Secretary of Defense for Acquisition and Sustainment. (2020). *Operation of the adaptive acquisition framework* (DoDI 5000.02). DoD. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.PDF

Office of the Under Secretary of Defense for Research and Engineering, & Office of the DoD Chief Information Officer. (2024, February 16). *Protection of mission critical functions to trusted systems and networks*. (DoDI 5200.44). DoD. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/520044p.pdf

Secretary of Defense. (2025, March 6). *Memorandum for senior pentagon leadership commanders of combatant commands defense agency and DOD field activity directors: Directing modern software acquisition to maximize lethality*. DoD. https://media.defense.gov/2025/Mar/07/2003662943/-1/-1/1/DIRECTING-MODERN-SOFTWARE-ACQUISITION-TO-MAXIMIZE-LETHALITY.PDF

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net