Department of Defense Software Modernization Strategy

Software will be the differentiator in the continued defense of our nation and is the building block for emerging technologies. It is a critical asset we must defend and an advantage we must exploit. DoD must take steps to lead in software modernization. The DoD Software Modernization Strategy is the first step, providing overarching principles, a common framework for understanding, and initial goals and objectives. It builds upon current momentum and leans on the invention and successes of DoD organizations. The Department, as an enterprise, must continue to work together to implement the vision of this strategy, deliver resilient software capability at the speed of relevance.

In implementing the vision, it cannot be overemphasized that the road ahead is bumpy, resources limited, and competition fierce. Success necessitates not just action, but an overall shift in mindset and culture. We must also lead this culture change, recognizing and instilling the notion that modernization is a perpetual journey ... one the Department must take to reinforce and guarantee the future of its warfighting dominance.

Contents

U.S. Department of Defense (DoD)

Stakeholder(s):

Kathleen H. Hicks :
Deputy Defense Secretary

DoD Organizations :
Software modernization requires a cohesive Departmental effort. Implementing the goals and objectives of this strategy involves the authorities of various DoD organizations.

DoD Software Modernization Coordinators :
The DoD Chief Information Officer (DoD CIO), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the Under Secretary of Defense for Research and Engineering (USD(R&E)) will lead the coordination of software modernization activities.

DoD Chief Information Officer

Under Secretary of Defense for Acquisition and Sustainment

Under Secretary of Defense for Research and Engineering

Digital Modernization Infrastructure Executive Committee :
Understanding fiscal realities, the DoD CIO, USD(A&S), and USD(R&E), under the direction of the Digital Modernization Infrastructure Executive Committee, will form a Software Modernization Senior Steering Group (SSG) to appropriately prioritize activities, and to develop and maintain an annual action plan to incrementally implement goals and objectives.

Software Modernization Senior Steering Group :
The SSG will develop performance metrics to measure progress against meaningful operational outcomes and reassess the action plan regularly to ensure that priorities and target activities remain relevant and of value. They will follow this strategy's publication with various guidance documents (e.g., policy, reference designs, and standards) to support implementation and ensure integration with other initiatives like JADC2, ZTA, and electromagnetic spectrum superiority. Additionally, they will establish a software capability portfolio to integrate activities, shape budgetary decisions, and ensure the smart investment of resources.

Vision

Software is the differentiator in the continued defense of our nation

Mission

To deliver resilient software capability at the speed of relevance

Values

Principles: Unifying Principles ~ The unifying principles of this strategy form the underlying basis of intent as the Department implements software modernization. These principles consider existing DoD strategies and maintain broader themes at the forefront, ensuring a holistic to include, but not be limited to, just a technical perspective.

Security: A Primacy of Security, Stability, and Quality at Speed - DoD must not allow the pendulum to move based strictly on the metrics of speed.

Stability: Resilient software must be defined first by execution stability, quality, and dependable cyber-survivability.

Quality

Rapidity: These attributes can be achieved at speed by aggressively adopting modern software development practices that effectively integrate performance and security throughout the software development lifecycle.

Intelligence: Cloud Smart/Data Smart - Cloud services and data are fundamental to software modernization.

Best Practices: Software must smartly utilize cloud services and incorporate data best practices to ultimately deliver impactful capabilities.

Data: DoD must accelerate cloud adoption to enable software modernization and proactively manage data following the DoD Data Strategy.

Cost-Effectiveness: Enterprise First - The Department's technical delivery is bound by fiscal realities that require an efficient and cost-effective portfolio. Enterprise capabilities are a critical part of the portfolio.

Stewardship: Collaborative stewardship of enterprise capabilities facilitates adoption and allows DoD Components to maximize value under constrained resources.

Collaboration

Inclusiveness: No One Left Behind - Software modernization introduces improved capabilities and greater automation.

Leadership: This modernization must be driven by strong leadership, powered by technical talent, and leveraged by an upskilled workforce.

Talent: As such, development, training, and recruiting of the Department's workforce are critical aspects of software modernization.

Comprehensiveness: More Than Code - Software modernization is more than just code development. It includes the many policies, processes, and standards that take a concept from idea to reality. Considerations such as contracting and intellectual property rights, as well as transition from development to fielding, are often overlooked and underappreciated.

Empowerment: These policies, processes, and standards must not hinder, but empower the vision of this strategy.

1. Cloud

Accelerate the DoD Enterprise Cloud Environment

The DoD Enterprise Cloud Environment is the foundation for software modernization. The multi-cloud, multi-vendor approach still holds true. The requirement for cloud across all classification domains, from enterprise to tactical edge, is still valid. The need to transition from disparate cloud efforts to a structured, integrated, and cost-effective cloud portfolio remains the Department's intent. Working with commercial cloud service providers continues to be critical as the Department technically evolves. DoD and commercial cloud service providers must work together to quickly and securely deploy cloud services and ensure transparency of cybersecurity activities to maintain the protection of DoD data. This goal is central to the President's Executive Order on Improving the Nation's Cybersecurity, Executive Order 14028, directing accelerated movement to secure cloud services and emphasizing the importance of commercial relationships.

1.1. Contracts

Mature an Innovative Portfolio of Cloud Contracts.

DoD must provide access to cloud services across the enterprise, maintaining parity with the commercial market. An innovative portfolio includes a meaningfully differentiated set of enterprise contracts that leverages existing acquisition success while avoiding duplication. The DoD acquisition community must work closely with industry to continuously improve contracting processes for cloud services, to ensure access to the full breadth of cloud security services, and to achieve a more holistic and diverse contract portfolio that benefits the entire DoD enterprise. Contractual delays impact DoD's competitive advantage and ultimately, place warfighters and their missions at risk.

1.2. Data

Secure Data in the Cloud.

Securing data in the cloud consists of two key thrusts: improving authorization processes and establishing DCO in the cloud. Securing cloud for the Department begins with Federal-level processes (i.e., FedRAMP) and proceeds with DoD-specific processes (i.e., provisional authorization) coupled with cooperative independent government cybersecurity test and evaluation. These processes establish a list of approved cloud service offerings that meet DoD security criteria. System or application security compliance processes (i.e., Authority to Operate) ensure the appropriate implementation of security controls within a DoD Component's risk tolerance. These processes must be coupled with independent government developmental and operational cybersecurity testing to enhance understanding of the operational-resilience of the system or application to hostile attacks. All of these authorization processes must be faster to deliver in an agile era without sacrificing security. Critical to managing cybersecurity risk is establishing DCO in the cloud. DCO must enable the Department to stay ahead of threats, discover vulnerabilities early, and respond to questionable behavior quickly, taking into account recurring cybersecurity test and evaluation. A coordinated response to cyber incidents in the cloud requires cooperation across DoD organizations and between DoD and industry. DoD must mature and deliver DCO capabilities, providing both technical capability and complementary incident reporting and response processes, to enhance our defensive posture.

1.3. Design Patterns

Accelerate Cloud Adoption through Automated Design Patterns.

Automation is a force multiplier for limited software talent and allows for the faster, more consistent adoption of cloud services. DoD must provide reusable automated design patterns, such as Infrastructure as Code, Compliance as Code, and hardened software containers, to ease the burden required in standing up and configuring virtual development environments. These automated design patterns must be available across the enterprise, integrated into authorization processes, and continuously updated and configuration controlled. They must be based on industry best practices and prescribed or recognized standards, as well as enable diverse implementation approaches. Use of these patterns across DoD promotes consistent and robust architecture, up-to-date security, and a faster path to deployment.

1.4. Infrastructure

Prepare OCONUS Infrastructure for Cloud.

DoD's strategic positioning outside the continental United States (OCONUS) is critical to maintaining a credible deterrent. As such, forces abroad must have access to the same, if not better, capabilities as those on the homefront. Cloud services OCONUS are fundamental to enabling a Joint Force capable of quickly and decisively mobilizing air, land, sea, space, and cyberspace capabilities in response to adversaries threatening the United States or our allies. DoD must improve OCONUS infrastructure, from facilities to networks, to fully take advantage of cloud services, enabling persistent warfighter access to data sources and producers.

2. Software Factory

Establish Department-wide Software Factory Ecosystem

As mentioned earlier, software increasingly defines military capabilities; therefore, DoD must scale its ability to produce secure and resilient software at speed to maintain a competitive advantage. This strategy recognizes that the modern approaches and tools, as well as the technical talent needed to do this, are not without cost. The Department must pursue an enterprise-wide approach, establishing a software factory ecosystem that takes advantage of investments already made by the Military Services (e.g., Air Force Platform One, Navy Overmatch Software Armory, Marine Corps Business Operations Support Services, and Army Coding Resources and Transformation Ecosystem) and scales their success to enable cross-Program/cross-Service use as espoused in the 2019 Defense Innovation Board Software Acquisition and Practices Report.

2.1. DevSecOps

Advance DevSecOps through Enterprise Providers.

DoD must establish requirements for a reasonable number of approved enterprise providers to efficiently scale software factories, minimize unnecessary platform duplication, and advance DevSecOps. DevSecOps platforms at scale must provide not only technical capability but the processes to attract and onboard customers (e.g., business operations model, sustainment model, and cybersecurity processes). This ecosystem of DevSecOps platforms must also provide a diversity of capability to address the Department's various mission scenarios.

Stakeholder(s):

Enterprise Providers

2.2. Software Deployment

Accelerate Software Deployment with Continuous Authorization.

Many DoD Components identify obtaining an Authority to Operate (A TO) as the longest step in developing and deploying software. Automation creates opportunities that allow DoD to reevaluate the A TO process, shifting authorization from a "check-the-box for hundreds of security controls" activity to a "continuous authorization" activity. Continuous authorization encompasses validating the quality and security of the software development platform, process, and platform team. It couples this validation with automation to produce real-time and continuous evidence, verifying the defensive posture of the platform and resulting software in real time. DoD's cybersecurity professionals must collaborate with software developers and system engineers to identify pipeline and process-generated evidence that verifies appropriate protections are in place for resilient and survivable software.

2.3. Tools

Drive Reciprocity of Tools with an Enterprise Repository.

Commercial tools are critical to software development and must be made available at a faster pace to a broader base of users. DoD cannot continue to reevaluate tools for each network domain, leading to both duplication of effort and delayed deployment. DoD must vet commercial tools once for cybersecurity purposes and make them instantly available to appropriate users through an enterprise-like repository.

2.4. Control Points

Streamline Control Points for Seamless End-to-End Software Delivery.

It cannot take months to deliver code from a software factory to an operational environment due to network access approval timelines or cybersecurity compliance processes. In providing software, control points and decision approvals at various organization and network boundaries must be streamlined and allow for the end-to-end delivery of software from a development environment to an operational domain.

2.5. Innovation

Speed Innovation into the Hands of the Warfighter.

With increasing reliance on technology across the world, DoD cannot allow digital infrastructure to become stale. The Department must evolve and innovate smartly, leveraging industry, academic, and scientific communities to drive toward technical solutions of mutual benefit, to establish creative relationships through agreements, and to foster experimentation. The science and technology community currently leverages academia and industry to drive technical breakthroughs but must couple this with an innovation pipeline that takes research efforts from pilot to operational capability at speed and scale.

Stakeholder(s):

Warfighters

3. Resilience & Speed

Transform Processes to Enable Resilience and Speed

The Department is an enterprise of enterprises with laws and processes governing the way it buys, implements, and operates across a vast and diverse set of missions. These processes, established in a different era, cannot keep pace with the changing impact of technology. To maintain the Department's warfighting dominance, DoD must take steps to begin transformation in how business is done.

3.1. Policy, Regulations & Standards

Evolve Policy, Regulations, and Standards.

DoD leadership must recognize the importance of software modernization through policy, regulations, and standards. With Congressional support, the Department is empowered to evaluate policy and guidance to address unnecessarily restrictive or misaligned compliance activities. Policy and guidance must consider topics such as software management, security, and open source. DoD must also establish appropriate boundaries without inhibiting the pursuit of new ideas. In addition to guidance, DoD must participate in industry and international standards bodies to ensure that adopted software standards benefit the collective global community.

3.2. Acquisition

Make Acquisition More Agile.

Efforts already underway continue to make the acquisition lifecycle and the funding of software programs more agile (e.g., Adaptive Acquisition Framework, a DoD software acquisition pathway, and a Congressionally-approved Budget Activity 8 (BA8) Software Research, Development, Testing and Evaluation Appropriation pilot program). DoD leaders must continue to pursue flexibility in the acquisition and funding of DoD software programs.

3.3. Software

Treat Software as Data.

Software may be a component of a system, a tool, or part of the infrastructure, and software code may also be considered a data asset to be managed and protected accordingly. Leveraging the DoD Data Strategy, DoD must ensure appropriate data access and appropriate data rights to develop, maintain, and protect software. DoD should partner with industry to create intellectual property strategies that better balance the return on investment interest of both DoD and software vendors. These strategies should emphasize the use of modular open systems approaches and negotiation of specialized licenses to ensure flexibility and agility in creating mutually beneficial business arrangements that recognize and distinguish DoD's roles as customer, co-investor, and co-developer.

3.4. Competencies

Advance Technical Competencies.

DoD's growing reliance on software, whether custom, as-a-service, or commercial-off-the-shelf (COTS}, requires new skillsets and a rebalance of talent (e.g., an increase in software developers and cyber warriors).

This talent is difficult to attract and retain. DoD must plan early for the needed skillsets of the future and update hiring processes, career development programs, and workforce incentives to build toward a workplace where the best want to serve and stay. The Military Services must work together to establish a standard and dynamic inventory of baseline training and augment that training with investments in cross-Service, on-the-job apprenticeship programs and rotation opportunities.

3.5. Workforce

Empower the Broader Workforce as Contributors to Technology.

Developers are not the only ones who can impact software modernization. From infrastructure managers to operators, the entire workforce has the opportunity to help evolve technology. The Department must drive toward a technology-literate workforce, not just the warfighter but all those who serve the various missions of defense. The entire workforce must understand their role in delivering software and find ways to streamline processes, push for automation, and better leverage technology.

3.6. COTS Software

Manage COTS Software for Efficiencies and Effectiveness.

As the Department modernizes its ability to develop software, it must also seek economies of scale through enterprise licenses, manage regular software updates and patches quickly in partnership with the testing community for continual improvements in security and performance, and provide access to proven software products to include their associated security technical implementation guides. Additionally, DoD must improve the visibility of and return on software investments, licenses, and overall inventory through robust software asset management practices for a cost-effective software portfolio.

3.7. Enterprise Services

lncentivize the Use of Enterprise Services.

The concept of enterprise services makes financial sense only if those services obtain widespread adoption. The Department must establish a more robust process for funding and resourcing enterprise services to deliver at or above the level required by the end user. DoD leaders must continue to work closely to identify financial enablers such as a working capital fund specific to software modernization or a standard business model that provides for competitive fees for service.

Administrative Information

Start Date: 2021-11-30
End Date:

Publication Date: 2022-05-18
Source: https://media.defense.gov/2022/Feb/03/2002932833/-1/-1/1/DEPARTMENT-OF-DEFENSE-SOFTWARE-MODERNIZATION-STRATEGY.PDF

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone:

PDF formatted using TopLeaf XML publisher
www.turnkey.com.au