DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB - 1 2022

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Software Modernization

Delivering a more lethal force requires the ability to evolve faster and be more adaptable than our adversaries. The Department's adaptability increasingly relies on software and the ability to securely and rapidly deliver resilient software capability is a competitive advantage that will define future conflicts. Transforming software delivery times from years to minutes will require significant change to our processes, policies, workforce, and technology.

To that end, I have approved the DoD Software Modernization Strategy (attached) and am directing the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment, and the Under Secretary of Defense for Research and Engineering to lead implementation of the strategy through the Software Modernization Senior Steering Group (SW Mod SSG). To ensure progress, the SW Mod SSG will deliver an implementation plan within 180 days and will oversee enterprise-wide progress reported through Business Health Metrics. These efforts include, but are not limited to:

- DoD Component execution of DoD CIO Capability Programming Guidance in support of DoD CIO budget certification for Cloud and development, security, and operations (DevSecOps) investments.

- Enterprise-wide implementation of innovative acquisition authorities and policies, to include DoD Instruction 5000.87, Operation of the Software Acquisition Pathway.

- Increased DoD Component utilization of software factories and secure DevSecOps pipelines.

The DoD Software Modernization Strategy provides the approach for achieving faster delivery of software capabilities in support of Department priorities such as Joint All Domain Command and Control and artificial intelligence. Given this requires the combined focus of DoD senior leadership, I expect all offices and personnel to provide the support necessary to make software modernization a reality.

Attachment:
As stated

Department of Defense Software Modernization Strategy

November 2021

Version 1.0

Foreword

"...running beneath many of these broad trends is a revolution in technology that poses both peril and promise. The world's leading powers are racing to develop and deploy emerging technologies...that could shape everything from the economic and military balance to the future of work..."

Interim National Security Strategic Guidance, March 2021

Five Years into the Future. A natural disaster has devastated critical infrastructure across a partner nation's seaboard, threatening U.S. assets. DoD is providing disaster relief assistance and deploys units to the region by sea and by land. Software detects the disaster and maneuvers cloud computing resources to the region dynamically. Response personnel deploy a push-button collaboration environment with enterprise security, compliance, and credentialing solutions in place within minutes. Collaboration across units is enabled, and data and communications flow securely and rapidly despite surrounding infrastructure damage.

Three Years into the Future. In theater, cyber warfare has become a retaliatory series of increasingly sophisticated and frequent attacks threatening to destabilize regional security, escalating responses into the kinetic realm. DoD software factories automatically and proactively deploy measures based on current and future threats to vulnerable systems, from fighter aircraft to communications equipment, enabling continued joint operations.

Today. A global pandemic has forced millions out of the office and into isolation. National Guard personnel are deployed to assist with vaccination rollout to the tune of 1.5 million doses per day. Collaboration, logistics, and communications software must be seamlessly acquired and securely scaled to support the Department's operations.

The Department's competitive advantage, today and tomorrow, is reliant on strategic insight, proactive innovation, and effective technology integration enabled through software capabilities. Software modernization, the ability to quickly deliver high-quality, secure software through reuse, acquisition, or custom development, must be part of the Department's DNA.

The DoD Software Modernization Strategy sets a path for technology and process transformation that will enable the delivery of resilient software capability at the speed of relevance. It is one in a set of sub-strategies of the DoD Digital Modernization Strategy and builds upon, evolves, and replaces the DoD Cloud Strategy. Given software's role and pervasiveness across all aspects of mission capabilities and supporting infrastructure, implementation success of this strategy will rely heavily on partnerships across the Department.

In this era of competition and race for digital dominance, we cannot settle for incremental change. The Department must join together to deliver software better and operate as a 21st century force.

Contents

1 Introduction

Now is the time to be bold.

Early innovators within the Department have mounted ambitious challenges to what were once conventional expectations for DoD software delivery. The DoD Software Modernization Strategy spearheads their legacy, identifying a vision, along with goals and objectives, with the purpose of delivering better software faster. The strategy targets the following outcomes:

- **Shift secure software delivery left through modern infrastructure and platforms.** The strategy recognizes the importance of technology in evolving how the Department delivers software. It emphasizes the importance of commercial partnerships through the adoption of cloud and establishes a new commitment toward a Department-wide approach for software factories.

- **Enable this shift through true process transformation and people development.** The internal processes of the Department do not readily enable the software delivery pace required to compete. DoD must review and modernize requirements, budget, acquisition, and security processes to take advantage of new approaches and technologies, ensuring not only speed, but better quality and protection. This transformation must be coupled with a focus on people and their contribution to software modernization success.

2 Software Modernization Vision

Deliver Resilient Software Capability at the Speed of Relevance

Defending our nation and ideals of freedom is no longer confined to traditional battlefields. Adversaries now target not just our military facilities, defensive assets, and soldiers, but also the networks, critical infrastructure, and individual citizens that support our way of life. Their weapon and/or target of choice – information and data. Their enabling means – software.

Software is everywhere. It is integrated into our homes; drives us to work; and defines our health, economic, and military capabilities. DoD increasingly relies on software for automation, decision making, and execution of action. Software capabilities create opportunities for efficiencies and innovation while at the same time, expose new attack surfaces and risks. Adversaries know this. They continue to invest in technology and talent, leveraging software capabilities to undermine our operations, threaten our infrastructure, and manipulate democracy.

Fighting and winning on the next battlefield will depend on DoD's proficiency to rapidly and securely deliver resilient software capabilities. This proficiency must empower the warfighter and cyber defenders with the latest innovations to better understand the battlefield, enable Joint All Domain Command and Control (JADC2) with automation and machine learning, and arm leaders with a decision advantage through the aggregation and processing of data. To accomplish this, the Department cannot rely on antiquated platforms and processes of the past, and cannot do it alone.

The vision for software modernization is simple – deliver resilient software capability at the speed of relevance. Resilience implies software that is high-quality and secure, able to withstand and recover in the face of challenging conditions. Speed of relevance implies the accelerated delivery needed to maintain a competitive advantage. The approach is practical – unify efforts across DoD and partner with industry-leading software institutions to produce a portfolio of best-in-class software capabilities enabled by DoD processes. These capabilities must augment and integrate with other infrastructure components to include Zero Trust Architectures (ZTA), electromagnetic spectrum capabilities, and a growing inventory of connected military devices. The following sections identify a set of principles to unify efforts, a framework to organize activities, and initial goals and objectives to set implementation direction.

3 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.

- **A Primacy of Security, Stability, and Quality at Speed** – DoD must not allow the pendulum to move based strictly on the metrics of speed. Resilient software must be defined first by execution stability, quality, and dependable cyber-survivability. 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.

- **Cloud Smart/Data Smart** – Cloud services and data are fundamental to software modernization. Software must smartly utilize cloud services and incorporate data best practices to ultimately deliver impactful capabilities. DoD must accelerate cloud adoption to enable software modernization and proactively manage data following the DoD Data Strategy.

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

- **No One Left Behind** – Software modernization introduces improved capabilities and greater automation. This modernization must be driven by strong leadership, powered by technical talent, and leveraged by an upskilled workforce. As such, development, training, and recruiting of the Department's workforce are critical aspects of software modernization.

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

4 Software Modernization Framework

There are multiple ways to obtain software: adopt existing applications and platforms available through DoD Component-sponsored capabilities; buy software or the components for developing software through traditional software licenses to include those for low-code/no-code platforms and cloud software-as-a-service subscriptions; or custom develop software, oftentimes for DoD-unique capabilities which may include complex systems of systems, simple web applications, or embedded code.

Regardless of how software is obtained, software delivery is not a one-and-done activity and actions that treat software this way are harmful and counter-productive. Whether adopted, bought, or created, all modern software approaches incorporate modular design tenets and automation to achieve speed and secure continuous delivery.

The Software Modernization Framework in Figure 1 identifies a minimum set of technical enablers and processes that must be addressed to modernize software delivery. It serves as a common lexicon and organizing construct for discussing and coordinating software modernization activities. It is not intended to be all-inclusive or final but instead serves as a guardrail to focus implementation. Its level of applicability depends on the approach taken in obtaining software as dictated by mission (i.e., adopt, buy, or create), complexity of software development (e.g., a simple website to a system of systems), and consideration for the software end user (e.g., warfighter, healthcare provider, or recruiter).

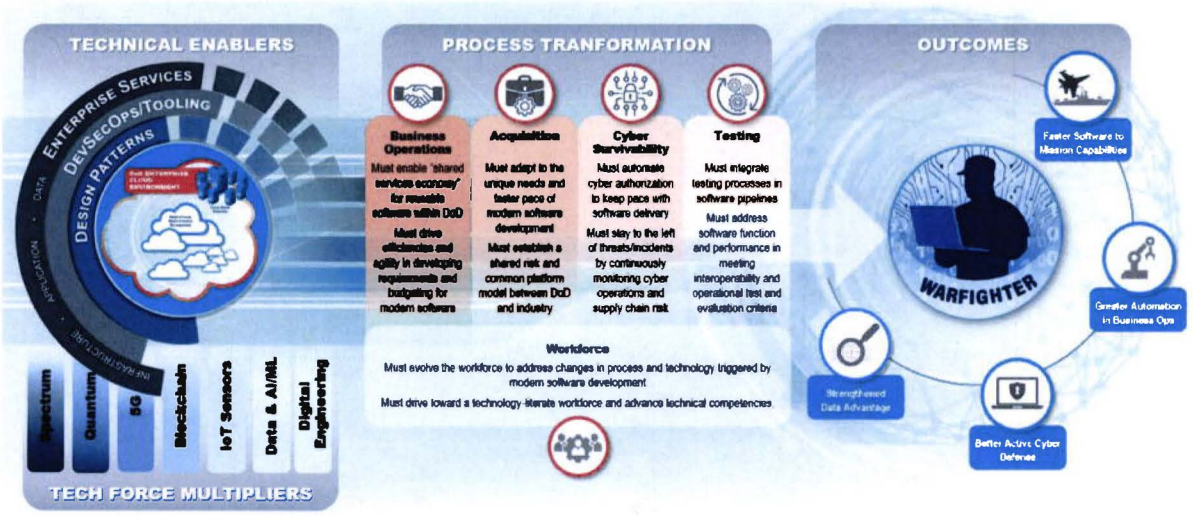

Figure 1: Software Modernization Framework

Technical Enablers: DoD must continuously adopt the latest technologies and approaches to deliver resilient software capability at the speed of relevance. These technical enablers address mission requirements, enable interoperability, and ensure security. Enablers depicted in the framework are not all inclusive and are not independent of each other. They are represented as concentric circles to indicate that these complementary capabilities must be integrated to achieve maximum value and that their evolution, just like software delivery, is continuous in nature.

- ***DoD Enterprise Cloud Environment*** – The DoD Enterprise Cloud Environment is a multi-cloud, multi-vendor ecosystem providing cloud services across the Department. Cloud services include infrastructure, platform, and software services. This environment remains

fundamental to software modernization, providing global compute and access to industry innovation at a rate unattainable by DoD alone. A structured approach in establishing and maintaining this environment promotes consistency in service quality, economies of scale, and avoidance of risk posed by cloud sprawl.

- ***Design Patterns*** – Design patterns are reusable solutions to commonly occurring problems within a given context in a software design. The automation of these design patterns accelerates secure cloud adoption and software development. The initial focus of this enabler are the common activities needed to stand-up a virtual environment, which includes security compliance scanning and access management. These design patterns can be automated through standard blueprints or templates. Use of these blueprints or templates promotes the execution of consistent architectures and configurations across the software development landscape and plays a critical role in enabling scale, interoperability, security, and faster time to mission.

- ***Development, Security, and Operations (DevSecOps)/Tooling*** – DevSecOps is an organizational software engineering culture and practice that aims at unifying software development, security, and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release and deliver, deploy, operate, and monitor. The benefits of adopting DevSecOps include reduced time from development to deployment, more robust security, and faster capability at the speed of relevance. DevSecOps/Tooling represents the set of capabilities enabling the continuous integration and delivery (CI/CD) of secure software as produced through a software factory. A software factory is a software assembly plant for development and integration that contains multiple pipelines, equipped with a set of tools, process workflows, scripts, and environments, to produce a set of software deployable artifacts with minimal human intervention. It automates the activities in the develop, build, test, release, and deliver phases and supports multi-tenancy. To realize the full benefit, these capabilities must effectively couple technology (e.g., tools and platforms) with process change (e.g., security authorization and testing).

- ***Enterprise Services*** – Enterprise services provide ready-to-use composable functions (e.g., security services, identity management, application programming interfaces, and data analytics) to support software modernization efforts. They allow DoD Components to rapidly adopt and use secure capabilities in support of mission requirements, thereby, freeing up limited talent for unique software features and innovation. Additionally, enterprise services are a mechanism for obtaining improved financial value; buy once and accessible to all.

Tech Force Multipliers: New and emerging technologies continually change the digital landscape. In adopting these tech force multipliers, leveraging the DoD Science and Technology Strategy, DoD must consider the impact to technical enablers and processes of software modernization. In reassessing technical enablers and processes, DoD cannot limit itself to current software development concepts but must be prepared to think differently under new parameters.

Process Transformation: The software modernization framework recognizes that processes must change to take advantage of new technology. These changes must consider not only pace and agility, but incentives to facilitate new behavior, policy updates to allow for innovation and experimentation, and a shift from software compliance to operational readiness. At DoD's scale, these changes should start small but allow for incremental growth and eventual enterprise adoption. Desired outcomes from transformation efforts include shortening acquisition timelines,

providing economic incentives to break down siloed business operations and independently-managed services, and reducing the lead time for cybersecurity compliance.

- ***Business Operations*** – DoD's internal economics must change to promote the adoption of shared software development platforms and reusable software. The drivers that lead to siloed operations and independently-managed services must evolve. There must be resource incentives to foster the sharing, reuse, and trust of software capabilities. This includes building incentives into requirements and budgetary processes as well as simplifying shared services transactions through better internal management operations.

- ***Acquisition*** – Software needs are evolving, and software updates occur more rapidly than ever. Current acquisition and contracting cycles are too slow and may result in potentially obsolete software. Software acquisition must continue to change to accommodate speed and agility. This change must occur by working with industry.

- ***Cyber Survivability*** – A compliance mindset may lead to a false sense of security. Cybersecurity should be the driver and compliance an outcome. DoD must shift from a cybersecurity "snapshot in time" compliance culture to a cybersecurity practitioner culture where automation, real-time continuous risk monitoring, including supply chain risk and rapid incident response, are the norm, and integrated into software development pipelines. System security engineering methods and practices must be identified early and leverage new technologies and approaches to streamline risk processes for software, to inform continuous authorization, and to enable Defensive Cyberspace Operations (DCO).

- ***Testing*** – As software plays a more significant role in weapons platforms and mission capabilities, robust software testing must be integrated into delivery pipelines and account for end-to-end mission thread evaluations. Software testing must not just run through scripts assessing software features and functions, but reflect operational scenarios to ensure expectations and thresholds for operational performance are met. In support of cyber-survivability, DoD must employ cooperative and adversarial penetration testing and persistent cyber testing during development, and recurring cyber testing during deployed operations to ensure proactive defense.

- ***Workforce*** – Modern software and delivery practices require shifts in DoD's workforce. Tuning algorithms for warfighting platforms at the tactical edge requires software talent; processing data with low-code/no-code platforms requires upskilled analysts; and the advent of software-defined robotics requires a flexible workforce with appropriate levels of development and engineering knowledge. DoD must attract and retain this workforce talent, hire talent into leadership positions, and initiate upskilling efforts to successfully compete. This shift requires not only changes in workforce process, but culture. Leaders and managers must think differently about careers, how people work together, and how to build workforce synergy across the Department because the software-defined future needs multi-disciplined individuals, a better bridge between communities of experts and operators, and a technology-literate Joint Force.

Outcomes: The ultimate outcome of technical enablers and process transformation is better capability to the warfighter faster. Resilient software will deploy to mission capabilities at a faster pace, business operations will be more efficient and effective through greater automation, real-time cyber defenses will stay to the left of threat, and software will enable a strengthened data advantage by promoting a data-centric, data-driven operating environment. The following section identifies the goals and objectives that provide initial implementation direction for achieving these outcomes.

5 Goals and Objectives

Software modernization goals represent long-term endeavors aimed toward achieving the vision. The objectives of each goal are near-term targets focused on the technical enablers and process transformation of the framework.

5.1 Goal 1: 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.

Objectives:

- ***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.

- ***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.

- ***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.

- ***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.

5.2 Goal 2: 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.

Objectives:

- ***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.

- ***Accelerate Software Deployment with Continuous Authorization.*** Many DoD Components identify obtaining an Authority to Operate (ATO) as the longest step in developing and deploying software. Automation creates opportunities that allow DoD to reevaluate the ATO 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.

- ***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.

- ***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.

- ***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.

5.3 Goal 3: 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.

Objectives:

- ***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.

- ***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.

- ***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.

- ***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.

- ***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.

- ***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.

- ***Incentivize 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.

6 Unified Implementation

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

7 Conclusion

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.

"…Whatever the cost, America will keep itself secure. But in the process, we must not, by our own hand, destroy or distort the American system. This we could do by useless overspending. I know one sure way to overspend. That is by overindulging sentimental attachments to outmoded military machines and concepts."

Dwight D. Eisenhower, 1958