Department of Defense

Software Modernization Implementation Plan Summary

March 2023

Executive Summary

The DoD Software Modernization Strategy challenged us to be bold…to lead the transformation of technology, process, and people in delivering resilient software capability at the speed of relevance. The DoD Software Modernization Implementation Plan is the follow-on call to action, aiming to establish capabilities that simplify the mechanics of software delivery, allowing teams to instead focus on creativity.

The DoD Software Modernization Implementation Plan describes 1) the flexible oversight foundation that will allow for the continuous planning and management of software modernization and 2) the FY23-24 priority tasks. The flexible oversight foundation consists of the Software Modernization Senior Steering Group (SSG), a dynamic task planning and management approach integrated with the DoD CIO budget certification process, and a means to assess progress leveraging the Deputy Secretary of Defense's Management Action Group Digital Modernization Business Health Metrics. The FY23-24 priority tasks are organized by tiers under the goals of the strategy and include descriptions, responsible organizations, and near-term milestones.

Ultimately, the DoD Software Modernization Implementation Plan postures DoD to fight and win on the future battlefield – which will depend on DoD's proficiency to deliver resilient software capabilities rapidly and securely. Success will require bold leadership; a Department-wide, collective effort; and passion to achieve a software-empowered DoD.

Table of Contents

Introduction

Purpose of Document

On February 1, 2022, the Deputy Secretary of Defense approved and signed the Department of Defense (DoD) Software Modernization Strategy, setting the Department on a path to deliver resilient software capability at the speed of relevance. The publication of the strategy included the requirement for an implementation plan due 180 days after date of signature. The DoD Software Modernization Implementation Plan provides a flexible governance mechanism to identify and prioritize software modernization activities as well as the initial set of implementation actions identified for FY23-24.

The DoD Software Modernization Strategy compels DoD to be bold in pursuing the following outcomes:

- Shift secure software delivery left through modern infrastructure and platforms. This outcome 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 workforce development. 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. From senior leadership to boots on the ground, being conversant with technology will be an increasing factor in mission success. Continuously learning with the latest tools, technologies, and processes while expanding organizational capabilities through competitive hiring of skilled individuals is critical.

The implementation tasks in this plan align to the three goals of the strategy:

1. Accelerate the DoD Enterprise Cloud Environment
2. Establish Department-wide Software Factory Ecosystem
3. Transform Processes to Enable Resilience and Speed

Intended Audience for Document

This document is designed to evolve the expectation, creation, and utilization of software across DoD. The intended audience includes those responsible for software strategy, developers and operators building and using software, and people interested in the journey to modernize DoD software. For leaders, mission owners, and program managers, it provides an overview on the intended way ahead. For software developers, infrastructure managers, and data stewards, it provides an understanding of the bigger picture and how software modernization implementation activities fit together. For those executing the strategy, it provides a Department-level governance construct and management approach that will drive implementation of existing efforts and help make new, proven ideas a Department-wide reality.

Scope of Document

The DoD Software Modernization Implementation Plan (I-Plan) describes the flexible oversight foundation established to continuously plan and manage software modernization tasks, allowing for both the tracking of progress through senior-level reporting and the accommodation of changes in alignment with strategic direction. The components of the oversight foundation include governance with representation across DoD, a dynamic task planning and management approach providing visibility of key initiatives, and a means to assess the progress of the I-Plan and its impact on the mission. The I-Plan identifies an initial set of high-priority tasks primarily focused on the common infrastructure, capabilities, and process transformations required to enable software modernization. This initial set of tasks aligns to the goals of the strategy, leans heavily on initiatives already underway, and is not meant to be all-inclusive. Task execution will rely heavily on partnerships across DoD Components and cooperation with industry.

Software modernization challenges are complex. Challenges include disparate technical infrastructures aligned to rigid organizational boundaries; processes geared toward mechanical as opposed to digital capabilities; and an ingrained culture based on this legacy environment. This complexity requires an incremental and focused approach. Establishing an oversight foundation allows for incremental and continuous implementation. Focusing on an initial set of tasks improves the potential for implementation success and return on investment from both a capability perspective and more importantly, a cultural one. This I-Plan captures a starting point, highlighting tasks for FY23-24. Continued management and tracking of implementation will occur using agile methods and the governance described herein.

Oversight Foundation

Governance

The Software Modernization Senior Steering Group (SSG) is the primary governance body for managing implementation of the DoD Software Modernization Strategy. The SSG is tri-chaired by the Offices of the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), and the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). It includes representation from across the DoD Components and is responsible for prioritizing and driving software modernization initiatives, leveraging the requirements, budget, and acquisition processes of the Department. The SSG guides and tracks tasks associated with the I-Plan through the Action Officer Working Group (AOWG). For specific tasks that require additional expertise, the SSG through the AOWG may establish a sub-working group or task force to develop a specific product. Once the product is delivered, the sub-working group or task force is stood down.

Task Planning and Management Approach

The DoD Software Modernization Strategy establishes the framework for planning. All planned and ongoing software modernization initiatives will align with and forward the progress of the goals and objectives of the strategy. Since implementation occurs at all levels of DoD, the SSG will manage initiatives in tiers with Tier 1 focused on priority tasks, Tier 2 on the supporting tasks of the priorities, and Tier 3 on those tasks managed at the DoD Component level.

The SSG will manage tasks through continuous collaboration and dynamic reporting via dashboards connected to the right data sources and metrics. The SSG will provide visibility of activities to the broadest audience for full transparency and participation.

FY23-24 Tasks

The FY23-24 Tier 1 tasks and associated Tier 2 tasks are organized by the goals of the DoD Software Modernization Strategy. These tasks are not listed in priority order and are subject to change based on the flexible oversight foundation provided by the SSG. Each Tier 1 task identifies a set of current or proposed metrics subject to change as implementation takes place. Each Tier 2 task identifies the Office(s) of Primary Responsibility (OPR), Office(s) of Collateral Responsibility (OCRs), a description of the task, and a key milestone to take place within the FY23-24 time period. More detailed and/or future milestones to include any risks or issues will be tracked by the SSG.

OPRs are the primary lead for the task, are responsible for coordinating amongst the OCRs, and are, ultimately, the organizations reporting progress through appropriate forums. OCRs are supporting organizations with roles and expertise in implementing the task.

G1 Goal 1: Accelerate the DoD Enterprise Cloud Environment

The DoD Enterprise Cloud Environment is the multi-cloud, multi-vendor ecosystem providing DoD Components with access to cloud services at all classification levels from enterprise to the tactical edge. Objectives include diversifying DoD Components' contractual access to cloud, ensuring security in the cloud, accelerating use of cloud services, building and training a cloud workforce, and enabling cloud adoption at the edge. The following tasks, taken together, further the Department's progress in accelerating adoption of the DoD Enterprise Cloud Environment.

G1.1 Tier 1: Increase adoption of enterprise-approved clouds

The mission value delivered from an advanced, resilient cloud-computing environment is directly related to the adoption and use of the cloud environment by the Department's IT programs and mission systems. Driving increased adoption of cloud environments to include adoption at the tactical edge requires DoD Components to rationalize their current systems environment, make cloud smart decisions, and optimize their IT investments to leverage cloud services throughout DoD. The Department will make improvements to portfolio management processes to include governance, requirements, and roles and responsibilities to enable rationalization. Ongoing IT portfolio management, rationalization activities, and cloud adoption will be tracked using the Department's enterprise IT management and budget systems, assessed during annual DoD CIO budget review processes, and reported through the Advana software modernization dashboard.

G1.1.1: Award the Joint Warfighting Cloud Capability (JWCC)

G1.1.2: Mature cloud service brokering functions

G1.2 Tier 1: Provide cloud edge capabilities

Cloud services outside the continental United States (OCONUS) are fundamental to enabling the Joint All Domain Command and Control (JADC2) vision. DoD Components must be able to deploy joint applications and systems to the tactical edge as a seamless global cloud. Edge computing must provide sufficient capacity, bandwidth, and access; consistent production environment configurations; and separate security boundaries with rapid approval processes. DoD must provide coordinated cloud services OCONUS and at the tactical edge to enable the warfighter with faster decision-making capabilities.

G1.2.1: Develop the OCONUS Cloud Technical Design

G1.2.2: Pilot the Joint Operational Edge (JOE) concept with the joint community

G1.2.3: Expand on-premises cloud to the tactical edge

G1.3 Tier 1: Modernize cloud environment for security and networking

The Department continues to pivot cybersecurity toward the principles of Zero Trust to include activities associated with securing the cloud and improving performance in alignment with NIST SP 800-207. A balance of protections at the perimeter, data, and application layers must ensure robust security and high-quality performance.

G1.3.1: Evolve Boundary Cloud Access Points (BCAPs) to a Zero Trust architecture

G1.3.2: Establish the Defensive Cyberspace Operations (DCO) capability

G1.3.3: Operationalize DCO with the CSSP community

G1.3.4: Modernize cloud endpoint security

G2 Goal 2: Establish Department-wide Software Factory Ecosystem

DoD software factories are collections of people, tools, and processes that enable teams to continuously deliver value by deploying software to meet the needs of a specific community of end users while enabling continuous rollout and cutting-edge cyber resilience. Software factory ecosystems are a multitude of related assets that support the operations, production, acquisition, and delivery of mission capabilities including data analytics, AI/ML, and advanced software technologies. They enable continuous user engagement to prioritize and refine desired requirements and features. To the maximum extent, they leverage automation to replace manual processes and increase the security of Development, Security, and Operations (DevSecOps) processes by reducing human-caused unintentional mistakes or malicious interference with the software integration and delivery process. They are also able to reach economies of scale by providing training through assimilation and replication of industry best practices. DoD continues to make progress in standing up the software factory ecosystem to deliver software at the speed of relevance. The following tasks, taken together, mature DoD's software factory ecosystem and identify pilots in the digital engineering domain to realize software factory value.

G2.1 Tier 1: Optimize and increase adoption of software factory ecosystem

Software factories and DevSecOps are still relatively nascent across the Department. However, continued collaboration and communications through the SSG and forums like the DevSecOps Community of Practice are increasing awareness and interest in leveraging existing software factories and establishing new ones. DoD must take a coordinated approach to grow this ecosystem based on a common tailorable baseline to ensure quality and efficient use of resources that provide solutions approved and encouraged, according to mission needs.

G2.1.1: Establish software factory criteria and metrics

G2.1.2: Inventory digital platforms and software factories

G2.1.3: Increase adoption of Infrastructure as Code (IaC)

G2.1.4: Implement pilot to provide Digital Engineering as a Service (DEaaS) via DoD software factory ecosystem

G2.1.5: Virtualize hardware to improve embedded software development

G2.1.6: Provide access to on-demand mission test resources

G2.2 Tier 1: Enable trust and sharing across DevSecOps organizations

The DoD software factory ecosystem delivers many different software capabilities that are production ready. In an ideal situation, numerous feedback loops throughout the development/ delivery process allow for high volume learning with end users well before the software enters the targeted operational environment. Across this ecosystem, digital platforms allow software factories to leverage development capabilities and improve quality and efficiency. This reuse of digital platforms is enabled by trust established through rigorous processes and testing (e.g., Software Quality, Software System Safety Level of Rigor, Software T&E Verification, Validation and Accreditation). The encouragement of trust and sharing across the ecosystem facilitates a culture of collaborative capabilities. The incremental products, software capability, and programmatic interfaces created by software factories will find utility across other software factories and potentially across missions. Standards for products and testing are necessary to give confidence across Authority to Operate (ATO) boundaries and to establish the standard body of evidence for Authorizing Officials to quickly approve software usage.

G2.2.1: Establish standards for containerized software

G2.2.2: Publish Software Bill of Materials (SBOM) Implementation Guidance for DoD

G2.2.3: Provide clear Agile Software and DevSecOps testing guidance

G2.3 Tier 1: Advance access to and interoperability of software capabilities and data

Software factories enable the rapid delivery of operational software. Building systems that incorporate capabilities from different software factories necessitates integration based on open interfaces. Following the lead of commercial best practices, DoD needs to adopt an Application Programming Interface (API) First methodology that allows operational systems to be integrated by design and new systems to rapidly incorporate enhanced products. Software and data connectivity must also include security (including Zero Trust), AI ready data, and classification considerations.

G2.3.1: Publish Application Programming Interface (API) strategy

G2.3.2: Publish API standards

G2.4 Tier 1: Drive software development innovation

Mission capabilities are increasingly defined by software. DoD must maintain a current and fresh perspective as advancements in technology drive greater abstraction through software, hiding complexities that could be exploited by adversaries. DoD must continue to stay at the forefront of research in software and software development, accelerating the development of artificial intelligence-enabling capabilities, identifying ways to disrupt and potentially propel the Department forward.

G2.4.1: Develop the Science and Technology Implementation Plan

G2.4.2: Enable Trust and Sharing Across DevSecOps Organizations

G3 Goal 3: Transform Processes to Enable Resilience and Speed

Software modernization is not just about technology. It also requires processes and people working in an organization with an outcome-focused, efficient learning mindset. Legacy processes defined for a different era of software and those mindsets that keep an organization locked into legacy processes will prevent software from fundamentally improving. For software modernization to be successful, mindsets must change. The following tasks focused on cybersecurity, acquisition, and workforce require a shift in mindset to transform policies and processes that will allow DoD to realize the full potential of software modernization.

G3.1 Tier 1: Implement continuous authorization

Obtaining an ATO is the longest and most costly step in developing and deploying software. Digital platform automation can provide data (or “telemetry”) that transparently shows every detail of a digital system needed for a comprehensive cybersecurity validation on a continuous basis. These capabilities fundamentally change how DoD assesses and accepts risks via ATOs. Recognizing this, the DoD Chief Information Security Officer (CISO) recently released continuous authorization guidance in accordance with the DoD DevSecOps Reference Design defining a continuous ATO (cATO) and its key competencies. DoD must continue to build on this guidance to make continuous authorization a reality.

G3.1.1: Publish cATO follow-on guidance

G3.1.2: Pilot cATO process and issue cATO

G3.2 Tier 1: Increase agility in acquisition implementation

The DoD acquisition community continues to work with the Defense Industrial Base (DIB), prime defense contractors, and service providers to improve, increase, and enable all aspects of the Software Acquisition Pathway. Recently, DoD updated DoDI 5000.02 to provide maximum agility across programs through six pathways. As an example, the newest pathway—the Software Acquisition Pathway—incorporates modern software practices such as Agile, DevSecOps, and Lean. Together, the pathways provide tailorable options for programs to utilize a single or multi-pathway approach based on mission need, increasing the delivery speed of warfighting and business capability with an emphasis on security. Because software is a vital part of almost all acquisitions, it is imperative that all the pathways address ways to improve software development and deployment. The Department will continue to collect metrics on program cost, schedule, and performance with an emphasis on improving data collection accessibility and time to deliver with the widespread adoption of AI.

G3.2.1: Collect metrics on use of the software acquisition pathway

G3.2.2: Promote software modernization across all acquisition pathways

G3.2.3: Collect agile software contracting best practices

G3.2.4: Collect cost data on agile software programs

G3.3 Tier 1: Develop and expand the digital workforce

Rapid advances in software engineering skills, technology, and modern software development practices (e.g., build/test/release automation, continuous delivery pipelines, and tools) have proven highly successful in a competitive marketplace. Ensuring the Department continues to advance cutting edge digital skills while creating a culture of continuous development is necessary to keep pace with change and meet mission needs. The development and expansion of the digital workforce aligns with strategic efforts outlined by the Department to include the 2023-2025 DoD Cyber Workforce Strategy. This work is critical as the digital workforce underpins the ability to achieve all aspects of this I-Plan.

G3.3.1: Unify ongoing workforce efforts

G3.3.2: Utilize data to modernize management of the digital workforce

G3.3.3: Recruit and retain world-class software talent

G3.3.4: Provide foundational software development, digital threat, artificial intelligence, and cyber training

Driving Action and Adoption

The SSG will oversee software modernization tasks through active governance and integration with the CPG, DoD CIO budget certification process, and DMAG business health metrics. However, real task execution and software modernization success will rely heavily on DoD Components who are performing the legwork associated with budget planning, coalition building, and product development as part of existing programs and projects. Software modernization is not a standalone effort – it does not have its own budget, dedicated resources, or program of record. It is an integral part of every mission and therefore, every mission is responsible for achieving the vision, “Deliver Resilient Software Capability at the Speed of Relevance.”

Delivering the tasks of this I-Plan alone will not be enough. Software modernization requires adoption…adoption of capabilities, tools, processes, and mindset. DoD Components must be incentivized to continuously rationalize their portfolio of applications and systems to adopt new capabilities. DoD is reinvigorating IT portfolio management to establish these rationalization incentives and to implement a process that enables continuous modernization.

This I-Plan is not the final statement on the Department’s software modernization activities. It is a communication mechanism to share an initial list of tasks and activities that are underway and leading the Department forward. The real work and dynamic management of tasks will occur through the established oversight foundation where all DoD organizations are welcome and encouraged to participate. The end result is an active process to prioritize and track activities through relevant metrics with representation by action officers and senior leaders that improves our ability to create, share, and deliver software to protect our nation.