U.S. Department of Defense

Software Modernization Implementation Plan FY25 – 26

Executive Summary

The DoD Software Modernization Strategy laid the groundwork for transforming how DoD delivers software, emphasizing speed and resilience. This updated DoD Software Modernization Implementation Plan outlines the path forward for FY25-26 by building on the progress achieved during FY23-24 and adding new focus areas.

This FY25-26 Implementation Plan positions the DoD to maintain its competitive edge in an increasingly software-defined battlespace. By transforming processes, empowering teams, and fostering innovation, we aim to deliver resilient software capabilities at the speed of relevance. Success hinges on continued leadership engagement, Department-wide collaboration, and a shared commitment to a software-empowered DoD.

Table of Contents

Background

The DoD Software Modernization Strategy, signed by Deputy Secretary of Defense (DSD) and published in February 2022, provides the approach for achieving faster delivery of software capabilities in support of Department priorities. In the strategy, the DSD asked 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 jointly lead the effort to implement the strategy through an implementation plan to "ensure progress".

The FY23-24 Software Modernization Implementation Plan focused on collective actions that enabled the DoD to modernize the infrastructure, platforms, processes, workforce skills, and DoD culture for delivering secure software to the warfighter. Of the initial forty-one (41) tasks identified in the FY23-24 implementation plan, twenty-seven (27) were accomplished, twelve (12) were carried over to the FY25-26 implementation plan, and two (2) were combined with other tasks in the FY25-26 implementation plan

Introduction

Software is a critical element of systems in the Department of Defense (DoD) and the ability to deliver software at the speed of relevance requires continued software modernization by executing the tasks identified in this FY25-26 implementation plan. These tasks are not all encompassing, and software modernization requires continued innovation throughout the Services and the other DoD components for the Department to realize its DoD Software Modernization Strategy.

Just like software, modernization is never done. DoD continues toward a future where artificial intelligence will help make common and complex software functions commodities. Software code will automatically create secure virtual environments for developing applications, will orchestrate the components of a continuous integration/continuous deployment (CI/CD) pipeline, and will free up people to focus on the unique and innovative software applications and systems that make warfighting capabilities truly cutting edge and responsible.

More than ever, it is critical that DoD continue to modernize software approaches and realize the vision of the DoD Software Modernization Strategy, "Deliver resilient software capability at the speed of relevance."

Purpose of Document

The DoD Software Modernization Implementation Plan, FY25-26, identifies the next set of tasks to further software modernization progress, building on FY23-24 accomplishments and leveraging knowledge management (KM) practices to incorporate lessons learned. By creating, sharing, using, and managing knowledge effectively, the plan ensures continuous improvement and informed decision-making. The tasks in the plan continue to align with the three goals of the DoD Software Modernization Strategy:

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

The purpose of this document is to provide assistance with multiple facets of the ecosystem such as better buying power though enterprise licensing agreements with software tool vendors, strengthening cybersecurity posture with Continuous Authorization to Operate (cATO), and removing financial barriers to operate in a cloud environment.

Intended Audience for Document

The intended audience for the DoD Software Modernization Implementation Plan, FY25-26, includes those responsible for their organization's software strategy, developers and operators building and using software, and leaders tracking the DoD software modernization journey.

Scope of Document

This version of the DoD Software Modernization Implementation Plan describes updates to the oversight foundation established in the FY23-24 version. It includes the next set of tasks to further ensure that software modernization progress is continued and accomplished in the FY25-26 timeframe. Task completion continues to rely on partnerships across DoD Components and cooperation with industry.

Alignment with Other Strategies and Implementation Plans

The DoD Software Modernization Implementation Plan, FY25-26, is not a stand-alone document. It aligns and strengthens other DoD strategies and implementation plans, leveraging the power of information technology (IT) capabilities across the Department. The implementation plan aligns with DoD's Fulcrum which is the Department's IT Advancement Strategy to optimize the use of innovative products, improve IT user experiences, and enhance operational effectiveness by identifying tasks that focus on modernizing weapons systems and legacy business systems, and improving financial operations with cloud and software factories. Additionally, the implementation plan includes regular reviews and updates to ensure that modernized systems continue to meet the evolving needs of the organization, which aligns with the Fulcrum Strategy's emphasis on continuous improvement and adaptation.

- Fulcrum: DoD IT Advancement Strategy
- DoD Zero Trust Strategy
- DoD Data Analytics and AI Adoption Strategy
- DoD Cyber Workforce Strategy and Implementation Plan
- DoD Software Science and Technology Strategy and Implementation Plan
- DoD Cloud FinOps Strategy
- DoD OCONUS Cloud Strategy
- DoD Records Strategy
- Application Program Interface Technical Guidance

Governance

The DoD Software Modernization Senior Steering Group (SW Mod SSG) is the primary governance body responsible for managing implementation of the DoD Software Modernization Strategy. It is tri-chaired by the Office of 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)). The SW Mod SSG will continue to guide and track tasks associated with the FY25-26 plan and coordinate the implementation of these tasks using the governance structure and agile tools and methods to track progress, manage new activities, and receive recommended solutions and strategies through the Action Officer Working Group (AOWG).

Task Planning and Management Approach

This version of the DoD Software Modernization Implementation Plan simplifies task breakout, identifying strategic-level tasks with tactical-level subtasks for each goal of the strategy. The SW Mod SSG will continue to manage tasks through regular updates and continuous collaboration using the processes and tools established for the FY23-24 plan.

FY25-26 Tasks

This section identifies the FY25-26 tasks 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 oversight foundation described in previous sections.

Goal 1: Accelerate the DoD Enterprise Cloud

The DoD Enterprise Cloud Environment is the enterprise multi-cloud, multi-vendor ecosystem providing DoD Components with access to cloud services at all classification from strategic level to the tactical edge. In FY23-24, DoD made significant progress in enabling acceleration of cloud with the award of the Joint Warfighting Cloud Capability (JWCC), which provides direct contract access to cloud services at competitive rates; the maturation of Military Department cloud management offices to drive and facilitate cloud adoption; the implementation of select Joint Operational Edge (JOE) nodes proving out the technical design for commercial cloud at the tactical edge; the expansion of on-premises cloud to the tactical edge (e.g., Stratus); and publication of security guidance to maximize security services offered by commercial cloud service providers. The JWCC contract now provides a foundation of direct contracting access to cloud services, allowing DoD to focus on secure, innovative use of cloud to deliver cutting-edge software capabilities to the warfighter.

1.1 Establish Other Contract Options for Cloud Innovation

Description:

JWCC provides access to large hyperscale cloud providers. However, small businesses and niche providers are also a significant source of innovation. DoD must provide access to these small businesses and niche providers to maximize innovation opportunities. This entails not only a mechanism for contracting but a business model that supports and incentivizes small businesses and niche providers to invest in the DoD mission.

Outcomes Upon Completion:

This task will provide a contract mechanism for accessing cloud- related small businesses. It will include a proposed business model that provides the right small business incentives.

Subtasks:

1.1.1 Develop Business Model/Incentives for Small Businesses

1.1.2 Develop Small Business Contract Acquisition

1.1.3 Award Small Business Cloud Contracts

1.2 Establish a FinOps Foundation for Smarter Use of Cloud

Description:

Now that DoD Components are in the cloud or proactively migrating to cloud, DoD must ensure the effective and efficient use of cloud. Today, DoD Components purchase cloud through various mechanisms (e.g., cloud service provider resellers, other available enterprise cloud contracts, and existing contracts via other direct costs), resulting in unique service pricing, inconsistent terms and agreements, and multiple management approaches for cloud services. This hinders DoD's visibility of cloud usage, cost, and impact. Adopting Financial Operations (FinOps) as a discipline provides DoD with an enterprise perspective to optimize cloud investments in alignment with mission need.

Outcomes Upon Completion:

This task will provide a strategic approach for implementing FinOps, an operational framework and cultural practice which maximizes the business value of cloud, enables timely data-driven decision making, and creates financial accountability through collaboration between engineering, finance, and business teams. The task includes the activities required to establish an enterprise dashboard that intuitively illustrates cloud cost, usage, and trends for better cloud investment decision making.

Subtasks:

1.2.1 Publish FinOps Data Standard

1.2.2 Implement DoD Cloud FinOps Strategy via Enterprise FinOps Capability Minimum Viable Product (MVP)

1.3 Develop Quick Track SaaS ATO Process

Description:

Maintaining our cybersecurity standards and leveraging reciprocity between system owners and authorizing officials is critical to accelerate and streamline the delivery of capabilities to the warfighter. With the growing number of Software-as-a-Service (SaaS) offerings and to ensure access to innovative solutions coming from both large and small businesses, DoD must establish an equitable ATO process that provides a lower barrier to entry and faster access to capability. The process must consider the SaaS business model, approaches for validating security enterprise-wide or promoting reciprocity, and the impact of Saas on core infrastructure components. The process must also establish a framework of responsibility to include addressing enterprise versus DoD Component roles in making Saas available at various classification levels.

Outcomes Upon Completion:

This task will provide a quick track SaaS ATO process or approach to enable access to more SaaS providers.

Subtasks:

1.3.1 Determine SaaS ATO Process Requirements

1.3.2 Pilot the SaaS ATO Process

1.3.3 Publish SaaS ATO Process Guidance

1.4 Enable OCONUS Cloud Use for Applications at the Edge

Description:

As DoD continues to expand access to cloud at the edge, there is a need to provide common services that allow for the streamlined delivery of software capability to the warfighter. OCONUS cloud must be supported by reliable connectivity, provide software services that facilitate development and deployment of applications at the edge, and enable use by mission partners since the U.S. rarely fights alone. The complexity of infrastructure integration and the policy/technical limitations at the tactical edge require careful planning in taking OCONUS cloud to the next level of capability. This next level must promote and align with modern software practices (e.g., DevSecOps) and implement zero trust principles.

Outcomes Upon Completion:

This task will result in reference designs for the underlying cloud mesh enabling the transport of data, common services to facilitate software development and deployment, and mission partner information sharing via cloud at the edge.

Subtasks:

1.4.1 Align to DoD CIO published Cloud Mesh Reference Design

1.4.2 Align to DoD CIO published Common Services Reference Design

1.4.3 Align to DoD CIO published Cloud-Based Mission Partner Environment Reference Design

1.5 Codify Modern CSSP Model for Enhanced Cloud Security

Description:

With DoD capabilities and data migrating to cloud, it is imperative that security in the cloud meets or exceeds DoD standards. DoD must continue to modernize its approach to cybersecurity, recognizing that cloud is now an extension of the DoD Information Network. The desired end state includes an ability to sense suspicious or anomalous operations in the cloud, know when a vulnerability exists or an incident occurs in real time, and be able to react accordingly to mitigate the risk. DoD needs to measure the performance of these abilities and Cybersecurity Service Provider (CSSP) capabilities to provide assurance in the modern cyber environment. DoD must codify a modern CSSP model that drives toward this end state to set the stage for further transformation.

Outcomes Upon Completion:

This task will deliver any related policies and guidance needed while working on the rewrite of DoDI 8530.01 that will codify a modern CSSP model.

Subtasks:

1.5 Rewrite DoDI 8530.01, Cybersecurity Activities Support Procedures

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. In FY23-24, DoD established a software factory ecosystem baseline with the more mature software factories proving the value of DevSecOps through software delivery results. The baseline included not only an initial inventory of software factories but guidance and tools to enable consistency in approach like the publication of API technical guidance and test and evaluation tools based on a DevSecOps approach. The next step in the software modernization journey is to scale and reproduce proven success across the Department, making the use of the software factory ecosystem the default by mission owners.

2.1 Scale the Adoption of Modern Software Practices

Description:
The DevSecOps platforms and software factories that are the tangible implementation of this modern software approach are still in the early stages of adoption as the cultural shift required to make this ecosystem mainstream is significant. Over the past two years, the MILDEPs have inventoried software factories and DevSecOps platforms and DISA has provided Infrastructure as Code for continuous integration/continuous deployment pipeline implementation. DoD must continue to scale success and bridge the right disciplines together (e.g., cybersecurity, test and evaluation, acquisition, and finance) to ensure end-to-end enablement and realization of the software modernization vision and adoption of software platforms and factories organized by domain (e.g., command and control applications). This includes driving and measuring the progress of adoption and establishing policy and guidance to codify the shift in roles and responsibilities needed for DevSecOps and a domain-organized approach

Outcomes Upon Completion:

This task will provide visibility of adoption through appropriate data and metrics captured in the DoD IT Portfolio Repository (DITPR) and a Catalog and policy guidance to ensure all authorities in the DevSecOps value stream enable quality and speed.

Subtasks:

2.1.1 Provide DevSecOps Adoption Analytics
2.1.2 Publish a DevSecOps Platform and Software Factory Catalog
2.1.3 Create communications plans for SWF synchronization
2.1.4 Provide DoD-wide Software Assurance Capabilities.

2.2 Provide Tools to Speed Software Development Productivity

Description:
Software developers and engineers continue to struggle through approval processes and red tape to obtain access to common development tools. This hinders productivity and delays the delivery of software capability. DoD governance must adjust regulations which hinder the talent pool from accessing the common tools needed to effectively develop software. This includes promoting the existing capabilities available (https://web.git.mil) as well as the increasing availability of data, analytics, and Al technologies, and providing access to the latest software development tools and services ensuring their secure and consistent use (e.g., digital engineering capabilities to improve code development; infrastructure as code and repositories at the Secret level to enable classified software development; and adherence to information, data, and records management best practices).

Outcomes Upon Completion:
This task will provide access to tools and capabilities that improve software development productivity.

Subtasks:

- *2.2.1* Provide access to software development tools and services
- *2.2.2* Oversee the implementation of digital engineering for software development
- *2.2.3* Provide Infrastructure as Code for all JWCC capabilities
- *2.2.4* Provide Infrastructure as Code for IL6
- *2.2.5* Provide web.git.mil at the Secret Level

2.3 Enable Software Interoperability through APIs

Description:
As software development continues to use modular design approaches and microservices, integration and interoperability will become increasingly complex. In FY22, DoD released its API Strategy for incorporation into acquisition programs. In FY23-24, DoD developed API technical and contracting guidance to promote a common approach to API development and use. The update to the API Technical Guidance (MVCR 2) will be published shortly. DoD must continue momentum for this activity by enabling adoption through supporting capabilities and training materials.

Outcomes Upon Completion:
This task will provide access to analytical tools, capabilities, and training materials including a standardized API catalog. It includes delivery of a testbed enabling an API implementation investigation and the testing of different techniques and different types of service interfaces (i.e., APIs) and delivery of training to program offices for delivering service interfaces and APIs.

Subtasks:

- *2.3.1* Conduct Minimum Viable Product (MVP) to prototype a standardized API catalog
- *2.3.2* Publish a standardized API catalog
- *2.3.3* Deliver an API Test Bed
- *2.3.4* Develop API Training Modules

2.4 Increase Use of Continuous Authorization to Operate (cATO) for Better, Timelier Security

Description:

Continuous Authorization to Operate (cATO) (defined in glossary) must become a standard business practice. This requires not only having sound criteria to issue a cATO, but building a community of Authorizing Officials who understand the criteria itself and can provide feedback into the process to better inform criteria requirements for sound risk decisions. DoD must continue to work with DoD Components to help software platforms mature their people, processes, and technology to obtain a cATO; issue cATOs to qualifying platforms; and educate Authorizing Officials on leveraging and trusting cATOs.

Outcomes Upon Completion:

This task will deliver additional platforms with cATOs, cATO analytics regarding adoption and impact, and training material for Authorizing Officials.

Subtasks:

2.4.1 Designate cATO Platforms

2.4.2 Provide cATO Analytics

2.4.3 Provide cATO Authorized Official Training Materials

2.5 Establish Software Factory Financial Operating Models

Description:

As software factories continue to mature, they are uncovering challenges associated with scaling operations, especially from a financial perspective. Across factories, financial operating models are inconsistent. DoD must provide guidance that establishes sustainable financial models for operating software factories to include the potential ability to fund software platforms and factories or components of this ecosystem as an enterprise service. If pursuing enterprise services, DoD must also reevaluate the enterprise funding model and policies to incentivize use of software ecosystem enterprise services Department-wide.

Outcomes Upon Completion:

This task will guidance regarding software factory financial operating models and propose a Software Ecosystem Enterprise Service funding model.

Subtasks:

2.5.1 Publish Software Factory Financial Operating Model Guidance

2.5.2 Propose a Software Ecosystem Enterprise Service Funding Model

2.5.3 Develop an approach to analyze the implementation of the Software Factor Financial Operating Model

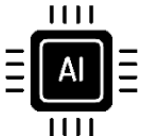
2.6 Prepare Software Factories for AI and Software-Based Automation

Description:

Software is the means for delivering AI models and automation capability. AI-related software must be constantly updated to account for the learning that takes place as AI senses and learns from its environment. Special considerations must be addressed by software factories delivering AI to include automated code generation, software tools or processes which will provide a means for ensuring data provenance, and guidelines that define AI traceability requirements. Risk assessment guides must inform the management of model data; management of the algorithm to avoid black box, bias, and integration issues; management of the underlying infrastructure to account for significant power and storage requirements; and sufficient testing mechanisms to validate operational and security functionality. DoD must get ahead of this need by establishing a DevSecOps AI deployment framework to transition smartly into the future.

Outcomes Upon Completion:

This task will provide a DevSecOps reference design that describes an AI deployment framework, in support of the DevSecOps process to train, test, deliver and deploy Large Language Models (LLM) and Artificial intelligence (AI).



Subtasks:

2.6.1 Identify a set of software tools or processes which will provide a means of enduring data provenance

2.6.2 Establish guidelines that define AI traceability requirements for GOTS and/or COTS software solutions

2.6.3 Construct a risk assessment guide that will be used to audit the safety of AI supporting infrastructure requirements

2.6.4 Determine AI Supporting Infrastructure Requirements

2.6.5 Publish DevSecOps Guidance for AI/ML Conduct Three AI Model to Production Pilots

Goal 3: Transform Processes to Enable Resilience and Speed

Software modernization is not just about technology. Delivering software at speed requires changing the way DoD does business. In FY23-24, DoD developed cATO evaluation criteria and implementation guidance to strengthen security, improve risk management, and accelerate cybersecurity approvals; continued to mature and increase adoption of the Software Acquisition Pathway; and introduced eight new software engineering work roles to the DoD Cyber Workforce Framework. DoD will continue with process transformation efforts to ensure an end-to-end approach for software delivery.

3.1 Evolve Policy, Regulations, and Standards

Description:

For modern practices to become the routine way of developing and delivering software, policy, regulations, and standards must be reviewed and updated. DoD must work with DoD Components to update policy and guidance to reduce the barriers to adopting new practices and to accelerate software delivery and cybersecurity approvals to enable adoption of the latest tools and services.

Outcomes Upon Completion:

This task will deliver updated policy and guidance related to software architectures, test and evaluation processes, and overall software management.

Subtasks:

- *3.1.1* Evolve Architecture Approaches for Software
- *3.1.2* Publish Software Modernization Policy
- *3.1.3* Provide Clear Software Agile and DevSecOps Testing Guidance
- *3.1.4* Provide Test and Evaluation Analytics and Updated Capabilities

3.2 Develop Secure Software Standards

Description:

Past and current cyberattacks elevate the need for secure software. In FY23-24, DoD integrated the National Institute of Standards and Technology Secure Software Development Framework into DoD guidance, "DevSecOps Fundamentals Guidebook: Activities and Tools," and rolled out software attestation and software bill of materials (SBOMs) requirements in alignment with Cybersecurity and Infrastructure Security Agency guidance, Executive Order 14028, and Office of Management and Budget Memo, M-22-18. DoD must continue to establish standards, processes, and capabilities to provide visibility into the software and services supply chain and to manage cybersecurity risk throughout the system lifecycle. This includes requiring software developers to meet or exceed performance metrics for following secure coding practices.

Outcomes Upon Completion:

This task will provide standards and capabilities for securing software throughout its lifecycle.

Subtasks:

3.2.1 Publish Secure Coding Practices and Metrics

3.2.2 Publish Secure Container Standards

3.2.3 Pilot SBOM Repository Capability

3.3 Modernize JCIDS for DevSecOps

Description:

When software development goes wrong, oftentimes the root cause is unclear requirements. Joint Requirements for DoD begin with Joint Capabilities Integration and Development System (JCIDS). In FY22, DoD made updates to JCIDS to account for the software acquisition pathway (SWP), but there are more software touch points beyond SWP that require a comprehensive review of JCIDS and how it should change in a DevSecOps world. DoD must update the joint requirements process for software capabilities to both streamline reviews and approvals and enable greater agility.

Outcomes Upon Completion:

This task will provide updated JCIDS guidance that integrates DevSecOps more thoroughly in the joint requirements process and will identify expected outputs and recommended metrics like DORA metrics.

Subtasks:

3.3.1 Provide Updated JCIDS Supplemental Guidance

3.3.2 Apply JCIDS Cyber Survivability Endorsement's Lessons Learned for DevSecOps in All Acquisition Pathways

3.4 Apply Modern Software Practices to Legacy Business Systems

Description:

The Office of the DoD CIO inherited the management of the Defense Business Systems (DBS) portfolio with the disestablishment of the Chief Management Officer. Upon inheritance, DoD CIO reinvigorated the Defense Business Council and established an approach for rationalizing DBS with a focus on driving out legacy systems that rely on aging infrastructure and codebase. The Department must retire or transform these legacy DBS into current capability that applies 21st century ways of developing and maintaining software.

Outcomes Upon Completion:

This task will provide a playbook and a testing environment for legacy system transformation to include application of that playbook to select legacy DBS.

Subtasks:

- *3.4.1* Publish Legacy Transformation Playbook
- *3.4.2* Provide Legacy Transformation Testing Environment Conduct Three DBS Transformations

3.5 Drive Software Modernization in Embedded Weapons Systems

Description:

DoD must modernize how we develop and deploy software for weapons platforms to meet the need for changing capabilities and winning the next fight. Weapons programs have unique challenges such as specialty certifications before fielding (e.g., safety, ATO, airworthiness, nuclear, material release) but these critical processes have not been modernized which hinders the speed of delivery. OUSD(A&S) launched the weapons ignite initiative for the software acquisition pathway (SWP) to engage leading weapons systems across the Military Services to deliver a toolkit of best practices that can be adopted to deliver safety-critical software capabilities faster and to enable more weapons programs to adopt the SWP.

Outcomes Upon Completion:

This task will provide a toolkit of best practices that can be adopted to deliver safety-critical software capabilities faster for SWP programs and to enable more weapons programs to adopt the SWP.

Subtasks:

- *3.5.1* Deliver Weapons Ignite Toolkit 1.0
- *3.5.2* Publish Weapons Ignite Memo
- *3.5.3* Deliver Weapons Ignite Toolkit 2.0

3.6 Accelerate Adoption/Impact of Software Acquisition Pathway

Description:

Delivering software at speed also requires acquiring software at speed. In FY23-24, DoD continued to promote the use of the software acquisition pathway (when appropriate to the application context) as defined in DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway." Programs adopting the software acquisition pathway increased at an annual rate of approximately 50% and accelerated delivery cadence to the end user. Work must continue to improve the use of the acquisition pathway through training, to better understand the impact through improved measures of progress, and to proactively facilitate modern software practices across all Adaptive Acquisition Framework pathways.

Outcomes Upon Completion:

This task will result in acquisition training, analytics to better understand software acquisition adoption/impact, and software acquisition guidance across the other Adaptive Acquisition Framework pathways.

Subtasks:

3.6.1 Provide Software Acquisition Modular Training

3.6.2 Improve Software Acquisition Analytics

3.6.3 Publish Software Acquisition Guidance for Other Pathways

3.7 Scale an Enterprise-level Software Cadre

Description:

Software is critical to nearly every mission, major system, and critical technology across the DoD. It is imperative that DoD have a cadre of personnel who are experts in software development, acquisition, and sustainment to improve the effectiveness of software programs and activities of the DoD. Congress recognized this and directed in the FY22 NDAA Section 836 to establish a software cadre. The software cadre will provide advice and assist with the adoption of modern software practices to accelerate software program office and related functional workforce learning curves, resulting in higher quality, more secure software deployed to the operational environment faster.

Outcomes Upon Completion:

This task will develop and initiate a concept for the multiorganizational resourcing of a centrally led software cadre capability to be employed on priority efforts.

Subtasks:

3.7.1 USD (A&S) to sign memo to establish the Software Cadre including a charter

3.7.2 Publish lessons learned and best practices

3.8 Develop and Track Software Engineering Talent

Description:

With eight new software engineering work roles in place, codified, and published in the DoD Cyber Workforce Framework (DCWF), DoD must associate those roles with billets to understand where the software talent is and is not. The existing software workforce may require a clear set of qualification standards and a catalog of certification, training, and educational opportunities to achieve the qualifications. In addition, DoD should maximize the opportunities for civilians to participate in developmental programs.

Outcomes Upon Completion:

This task will identify where software talent exists and lead to informed enterprise decisions on qualification standards and opportunities for certification, training, education, and opportunities for participation in developmental programs.

Subtasks:

- *3.8.1* Increase Department Participation Coding Software Engineering Work Roles
- *3.8.2* Enter Software Engineering Work Roles in Personnel Systems of Record
- *3.8.3* Increase Participation in Civilian Development Programs

3.9 Drive Broader Adoption of Enterprise Software Licensing

Description:

The DoD Enterprise Software Initiative (ESI) proved that the Department can achieve cost avoidance when purchasing IT through enterprise Blanket Purchase Agreements (BPAs) and Enterprise Software Agreements, which provide discounted prices for decentralized ordering. As the Department continues to become more reliant on software products, both as components of software development and software-as-a-service, it becomes even more necessary to pool Departmental buying power together to keep costs reasonable. DoD must improve its visibility of software licenses to better negotiate future contracts, continue to provide enterprise licensing agreements for widely used software products, and constantly assess the vendor environment for new tools and capabilities to reinforce market competition.

Outcomes Upon Completion:

This task will provide a policy for managing software licenses and enterprise license agreements for software products.

Subtasks:

- *3.9.1* Publish Enterprise Licensing Policy
- *3.9.2* Publish Annual Enterprise Software Agreement Plan
- *3.9.3* Provide Enterprise License Agreements for Software Products

Maintaining Momentum

The SSG will continue to oversee software modernization tasks through active governance, collaboration with DoD Components, and integration with appropriate DoD decision and reporting processes. The tasks in this plan are intended to maintain momentum for progress and culture change as driven from the top through the development of policy, standards, and guidance, and the promotion and execution of enterprise-level processes and capabilities. However, realization of progress and culture change occurs at the DoD Component level. Departmental success relies on those government change agents and their industry partners who take strategic guidance and implementation plans and turn them into real capability directly benefiting the warfighter. These people do not talk or write about modernization; they actually do it. These are the people who inspire…who will take DoD to the next level of capability with their creativity, resourcefulness, and smart risk-taking mind-sets. It is because of these people that the Department will maintain modernization momentum. And it is this momentum that will keep the Department at the cutting edge of technology and at the forefront of military power.

Appendix A: Glossary

Term	Definition
Application Programming Interfaces (APIs)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. (NIST Information Technology Laboratory, https://csrc.nist.gov/glossary/term/application_programming_interface)
Continuous Authorization to Operate (cATO)	Continuous Authorization to Operate (cATO) is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system's cyber posture.
Container	A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container. (National Institute of Standards and Technology, (NIST))
DoD Software Factory	A collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end-users. It leverages automation to replace manual processes.
Infrastructure asCode (IaC)	The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files. (National Institute of Standards and Technology, (NIST. SP.800-204C))
Modern Software Development Practices	Practices (e.g., lean, agile, DevSecOps) that focus on rapid, iterative development and delivery of software with active user engagements. Small cross-functional software development teams integrate planning, design, development, testing, security, delivery, and operations with continuous improvement to maximize automation and user value. (DoDI 5000.87)
Minimum Viable Product (MVP)	A minimum viable product is an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on. Insights from MVPs help shape scope, requirements, and design. (DoDI 5000.87)
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (NIST SP 800-145, SP 800-145, The NIST Definition of Cloud Computing I CSRC)

Term	Definition
Zero Trust	Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. (NIST SP 800-270, https://csrc.nist.gov/publications/detail/sp/800-207/final)

Appendix B: Mapping of Goals, Objectives, and Tasks

Goal 1: Accelerate the DoD Enterprise Cloud Environment	
Objectives	Tasks and Subtasks
Mature an Innovative Portfolio of Cloud Contracts	(FY23-24) Increase adoption of enterprise-approved clouds
	Award the Joint Warfighting Cloud Capability
	Mature Cloud Service Brokering Functions
	(FY25-26) Establish Other Contract Options for Cloud Innovation
	Develop Business Model/Incentive for Small Businesses
	Develop Small Business Contract Acquisition
	Award Small Business Cloud Contracts
	(FY25-26) Establish a FinOps Foundation for Smarter Use of Cloud
	Publish FinOps Data Standard
	Publish FinOps Data Standard
Secure Data in the Cloud	(FY23-24) Modernize Cloud Environment for Security and Networking
	Evolve Boundary Cloud Access Points to a Zero Trust Architecture
	Establish the Defensive Cyberspace Operations Capability
	Operationalize DCO with the CSSP community
	Modernize cloud endpoint security
	(FY25-26) Develop Quick Track Software-as-a-Service (SaaS) ATO Process
	Determine Saas ATO Process Requirements
	Pilot the Saas ATO Process
	Publish Saas ATO Process Guidance
	(FY25-26) Codify Modern CSSP Model for Enhanced Cloud Security
	Rewrite DoDI 8530.01, Cybersecurity Activities Support Procedures
Accelerate Cloud Adoption through Automated Design Patterns	(FY23-24) Optimize and increase adoption of software factory ecosystem
	Increase adoption through Infrastructure as Code (laC)
	Expand DoD laC to support all JWCC Capabilities
Prepare OCONUS Infrastructure for Cloud	(FY25-26) Enable OCONUS Cloud Use for Applications at the Edge
	Align to DoD CIO published Cloud Mesh Reference Design
	Align to DoD CIO published Common Services Reference Design
	Align to DoD CIO published Cloud-based Mission Partner Environment Reference Design

Goal 2: Establish Department-wide Software Factory Ecosystem	
Objectives	Tasks and Subtasks
Advance DevSecOps through Enterprise Providers	(FY23-24) Optimize and increase adoption of SWF ecosystem
	Establish SWF criteria and metrics
	(FY25-26) Scale the Adoption of Modern Software Practices
	Provide DevSecOps Adoption Analysis
	Publish a DevSecOps Platform and Software Factory Catalog
	Create communications plan for SWF Synchronization
	Provide DoD-wide Software Assurance Capabilities
	(FY25-26) Establish a FinOps Foundation for Smarter Use of Cloud
	Publish FinOps Data Standard
	(FY25-26) Establish SWF Financial Operating Models
	Publish SWF Financial Operating Model Guidance
	Propose a Software Ecosystem Enterprise Service Funding Model
	Develop an approach to analyze the implementation of the Software Factory Financial
	Operating Model
	(FY25-26) Provide Tools to Speed Software Development Productivity
	Provide Infrastructure as Code for all JWCC Capabilities
	Provide Infrastructure as Code for IL6
Accelerate Software Deployment with Continuous Authorization	(FY23-24) Implement continuous authorization (cATO)
	Publish cATO follow-on Guidance
	Pilot cATO process and issue cATO
	(FY25-26) Increase Use of cATOs for Better, Timelier Security
	Designate cATO Platforms
	Provide cATO Analytics
	Provide cATO Authorized Officials Training Materials
Drive Reciprocity of Tools with an Enterprise Repository	(FY25-26) Provide Tools to Speed Software Development Productivity
	Provide access to software development tools and services
	Provide web.git.mil at the Secret Level
Streamline Control Points for Seamless End-to-End Software Delivery	(FY23-24) Optimize and increase adoption of SWF Ecosystem
	Implement Pilot to Provide Digital Engineering as a Service
	Virtualize Hardware to Improve Embedded Software Development
	Provide Access to On-demand Mission Test Resources
Speed Innovation into the Hands of the Warfighter	(FY23-24) Drive software development Innovation
	Develop the Software Science and Technology Implementation Plan
	Enable trust and sharing across DevSecOps orgs (JFAC Portal)
	(FY25-26) Provide Tools to Speed Software Development

Goal 2: Establish Department-wide Software Factory Ecosystem, Continued	
Objectives	Tasks and Subtasks
Speed Innovation into the Hands of the Warfighter, Continued	Oversee the implementation of Digital Engineering for Software Development
	(FY23-24) Advance access to and interoperability of software capabilities and data
	Publish Application Programming Interface (API) Strategy
	Publish API Standards
	(FY25-26) Enable Software Interoperability through APIs
	Conduct pilot to prototype an API catalog
	Publish a standardized API Catalog
	Provide an API Test Bed
	Provide API Training Modules
	(FY25-26) Prepare SWFs for Al and Software-based Automation
	Identify a set of software tools or processes which will provide a means of enduring data provenance
	Establish guidelines that define Al traceability requirements for GOTS and/or COTS software solutions
	Construct a risk assessment guide audit the safety of Al systems incorporated into a Software Factory
	Determine Al Supporting Infrastructure Requirements
	Publish DevSecOps Guidance for Al/ML
	Conduct Three Al Model to Production Pilots

Goal 3: Transform Processes to Enable Resilience and Speed	
Objectives	Tasks and Subtasks
Evolve Policy, Regulations, and Standards	(FY23-24) Enable Trust and Sharing Across DevSecOps Organizations
	Establish Standards for Containerized Software Publish DoD Software Bill of Materials Implementation Guidance
	Provide clear Agile Software and DevSecOps Testing Guidance
	(FY25-26) Evolve Policy, Regulations, and Standards
	Evolve Architecture Approaches for Software Publish Software Modernization Policy
	Provide Clear Software Agile and DevSecOps Testing Guidance
	Test and Evaluation Analytics and Updated Capabilities
	(FY25-26) Develop Secure Software Standards
	Publish Secure Coding Practices and Metrics
	Publish Secure Container Standards
	Pilot SBOM Repository Capability
	(FY25-26) Modernize JCIDS for DevSecOps
	Provide Updated JCIDS Supplemental Guidance
	Apply JCIDS Cyber Survivability Endorsement's Lessons Learned for DevSecOps in All Acquisition Pathways

Goal 3: Transform Processes to Enable Resilience and Speed, Continued	
Objectives	Tasks and Subtasks
Evolve Policy, Regulations, and Standards, Continued	(FY25-26) Apply Modern Software Practices to Legacy Systems
	Publish Legacy Transformation Playbook
	Provide Legacy Transformation Testing Environment
	Conduct Three DBS Transformations
	(FY25-26) Drive Software Modernization in Embedded Weapons Systems
	Provide Weapons Ignite Toolkit 1.0
	Publish Weapons Ignite Memo
	Provide Weapons Ignite Toolkit 2.0
Make Acquisition More Agile	(FY23-24) Increase Agility in Acquisition Implementation
	Collect metrics on use of the Software Acquisition Pathway
	Promote Software Mod across all Acquisition Pathways
	Collect Agile Software Contracting Best Practices
	Collect Cost Data on Agile Software Programs
Treat Software as Data	
Advance Technical Competencies	(FY23-24) Develop and Expand the Digital Workforce
	Unify Ongoing Workforce Efforts
	Utilize Data to Modernize Management of the Digital Workforce
	Recruit and Retain World-class Software Talent
	Provide Foundational SW Dev, Digital Threat, AI, and Cyber Training
	(FY25-26) Scale an Enterprise-level Software Cadre
	Memo signed by USD(A&S) to establish the Software Cadre including a Charter
	Publish Lessons Learned and Best Practices
	(FY25-26) Develop and Track Software Engineering Talent
	Increase Department Participation Coding Software Engineering Work Roles
	Enter Software Engineering Work Roles in Personnel Systems of Record
	Increase Participation in Civilian Development Programs
Empower the Broader Workforce as Contributors to Technology	
Manage COTS Software for Efficiencies and Effectiveness	(FY25-26) Drive Broader Adoption of Enterprise Software Licensing
	Publish Enterprise Licensing Policy
	Publish Annual Enterprise Software Agreement Plan
	Provide Enterprise License Agreements for Software Products
Incentivize the Use of Enterprise Services	

Appendix C: Alignment with Fulcrum Strategy

			Fulcrum														
			LOE 1: Provide Joint Warfighting IT capabilities to expand strategic dominance of US Forces & Mission Partners				LOE 2: Modernize information networks and compute to rapidly meet mission and business needs			LOE 3: Optimize IT Governance to gain efficiencies in capability delivery and enable cost savings				LOE 4: Cultivate a premier digital workforce ready to deploy emerging technology to the Warfighter			
Software Modernization Implementation Plan, FY25-26			1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4
	Goal 1: Accelerate the DoD Enterprise Cloud Environment	1.1						■									
		1.2								■	■						
		1.3			■								■				
		1.4	■	■				■									
		1.5							■								
	Goal 2: Establish Department- wide Software Factory Ecosystem	2.1	■										■				
		2.2	■	■					■			■	■				
		2.3		■							■						
		2.4			■				■				■				
		2.5										■					
		2.6			■						■						
	Goal 3: Transform Processes to Enable Resilience and Speed	3.1								■	■		■				
		3.2		■	■				■								
		3.3			■					■							
		3.4			■							■					
		3.5			■												
		3.6										■	■				
		3.7													■		
		3.8												■	■		■
		3.9								■			■				

Appendix D: Results of FY 23-24 Software Modernization Implementation Plan

I-Plan ID	Goal / Task / Subtask	Result
Goal 1: Accelerate the DoD Enterprise Cloud Environment		
1.1	Increase adoption of enterprise-approved clouds	
1.1.1	Award the Joint Warfighting Cloud Capability (JWCC)	Completed
1.1.2	Mature cloud service brokering functions	Completed
1.2	Provide cloud edge capabilities	
1.2.1	Develop the OCONUS Cloud Technical Design	Completed
1.2.2	Pilot the Joint Operational Edge (JOE) concept with the joint community	Completed
1.2.3	Expand on-premises cloud to the tactical edge	Completed
1.3	Modernize cloud environment for security and networking	
1.3.1	Evolve BCAPs to a Zero Trust architecture	OBE
1.3.2	Establish the Defensive Cyberspace Operations (DCO) capability	Carryover
1.3.3	Operationalize DCO with the CSSP community	Carryover
1.3.4	Modernize cloud endpoint security	OBE
Goal 2: Establish Department-wide Software Factory Ecosystem		
2.1	Optimize and increase adoption of software factory ecosystem	
2.1.1	Establish software factory criteria and metrics	Carryover
2.1.2	Inventory digital platforms and software factories	Completed
2.1.3	Increase adoption of Infrastructure as Code (Ia C)	Completed
2.1.4	Implement pilot to provide Digital Engineering as a Service (DEaaS)	Carryover
2.1.5	Virtualize hardware to improve embedded software development	Completed
2.1.6	Provide access to on-demand mission test resources	Completed
2.2	Enable trust and sharing across DevSecOps organizations	
2.2.1	Establish standards for containerized software	Completed
2.2.2	Publish Software Bill of Materials (SBOM) Implementation Guidance for DoD	Carryover
2.2.3	Provide clear Agile Software and DevSecOps testing guidance	Carryover
2.3	Advance access to and interoperability of software capabilities and data	
2.3.1	Publish Application Programing Interface (API) strategy	Completed
2.3.2	Publish API standards	Completed

Goal 2: Establish Department-wide Software Factory Ecosystem, Continued		
2.4	Drive software development innovation	
2.4.1	Develop the Science and Technology Implementation Plan	Completed
2.4.2	Enable trust and sharing across DevSecOps Organizations	Completed

Goal 3: Transform Processes to Enable Resilience and Speed		
3.1	Implement continuous authorization	
3.1.1	Publish cATO follow-on guidance	Completed
3.1.2	Pilot cATO process and issue cATO	Carryover
3.2	Increase agility in acquisition implementation	
3.2.1	Collect metrics on use of the software acquisition pathway	Completed
3.2.2	Promote software modernization across all acquisition pathways	Carryover
3.2.3	Collect agile software contracting best practices	Completed
3.2.4	Collect cost data on agile software programs	Carryover
3.3	Develop and expand the digital workforce	
3.3.1	Unify ongoing workforce efforts	Completed
3.3.2	Utilize data to modernize management of the digital workforce	Completed
3.3.3	Recruit and retain world-class software talent	Completed
3.3.4	Provide software development, digital threat, AI/ML, and cyber training	Completed


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA