Department of Defense
Software Science and Technology Strategy
Implementation Plan

August 2024

Office of the Under Secretary of Defense
for Research and Engineering

Washington, D.C.

DoD Software Science and Technology Strategy Implementation Plan
August 2024

Office of Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd-sea@mail.mil
https://www.cto.mil/sea/

Approved by

Principal Deputy Executive Director for Systems Engineering and Architecture

Office of the Under Secretary of Defense for Research and Engineering

August 2024

DoD Software S&T Implementation Plan Change Record

Date	Change	Rationale

Contents

Figures

Tables

1 Introduction

1.1 Purpose

This Department of Defense (DoD) Software Science and Technology (S&T) Implementation Plan (I-Plan) is a follow-on to the DoD Software S&T Strategy published by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) in 2021. The strategy responded to the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 Section 255 and outlined four goals:

- **Goal 1 – Shift Engineering and Development Left:** Address transition concerns earlier in the acquisition life cycle and align S&T initiatives (budget activity codes 6.1, 6.2, 6.3 (DoDI 7000.14-R Vol 2B)) with operational needs through strong collaborative teaming between DoD research scientists and the engineering community.
- **Goal 2 – Adopt an Integrated Framework of Shared Resources:** Advocate for research into shared resources to increase collaboration and reuse to prevent redundant stovepipe development.
- **Goal 3 – Transform the S&T Workforce:** Accelerate the use of new technologies to enhance the development, retention, identification, and recruitment of a superior S&T and engineering workforce.
- **Goal 4 – Align Software S&T with Acquisition:** Remove unnecessary barriers that inhibit, delay, or prevent software from S&T projects from transitioning into operations and delivering needed capability.

The DoD Software S&T Senior Steering Group (SW S&T SSG), a cross-functional team tri-chaired by OUSD(R&E), OUSD for Acquisition and Sustainment (A&S), and the DoD Deputy Chief Information Officer (CIO) for Information Enterprise, leads activities and coordinates implementation of the four goals. The SSG prepared this I-Plan.

The SSG will revise the details of this plan continuously to track progress and will plan to circulate cumulative revisions on cycles of 6 months to a year.

1.2 Audience

This document is designed to help coordinate S&T investment across DoD and maintain alignment with future warfighting needs and priorities. The intended audience includes those responsible for investment in software-related research and the transition of that research into fielded systems. For those responsible for developing and funding research initiatives, it provides insight into the priorities and advances needed to address specific gaps. For those transitioning research results into practice, it provides a guide to ongoing and planned research that may become candidates for prototyping and subsequent deployment at scale. For those planning research and development (R&D) of software-enabled capabilities, it provides awareness of a rapidly growing base of enterprise resources such as cloud infrastructure and software factory assets that can speed the development and delivery of research results to help research initiatives cross the software “valley of death” from research result to operational deployment.

In developing this plan, the SSG also seeks to coordinate policy and guidance across not only OUSD(R&E) but also OUSD(A&S) and the corresponding offices among the Military Services that direct S&T efforts and corresponding A&S activities.

1.3 Scope

Following this introduction, Section 2 of this I-Plan describes a flexible oversight approach to continuously plan and synchronize software-related S&T efforts, allowing for both the tracking of progress through senior-level reporting and the accommodation of changes to align with DoD strategic direction. The oversight approach will include governance with representation from across DoD, providing visibility into implementation initiatives and a means to assess the progress of the I-Plan and its impact on the mission.

Section 3 provides an initial set of high-priority tasks primarily focused on the common infrastructure, capabilities, and process transformations required to deliver software capability at the speed of relevance. To create the list, the SW S&T SSG asked DoD S&T organizations for examples of S&T efforts either planned or under way that align with the DoD Software S&T Strategy (2021) goals. The organizations contributed descriptions of the tasks and milestones, which the SSG reviewed and organized into the descriptions. The tasks lean heavily on initiatives already under way and are not meant to be all-inclusive. DoD Components and partners in industry are collaborating to execute the tasks.

The two appendices provide a matrix cross-referencing I-Plan tasks to the focus areas enumerated in the Software S&T Strategy and the language from NDAA FY 2020 Section 255 for reference.

1.4 Related Documents

This document is part of a series that describe the DoD's strategic activities related to software modernization:

- DoD Software Modernization Strategy (DoD 2021): The strategy "sets a path for technology and process transformation that will enable the delivery of resilient software capability at the speed of relevance" (page ii). It emphasizes the use of modern software technologies to deliver software capabilities at the speed of relevance, marking a transformation from the Department's traditional multi-year software acquisition timelines.
- DoD Software Modernization Implementation Plan (DoD CIO 2023): As a follow-on to the DoD Software Modernization Strategy, the implementation plan describes:

  > (1) the flexible oversight foundation that will allow for the continuous planning and management of software modernization and 2) the FY 2023-2024 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 FY 2023-2024 priority tasks are organized by tiers under the goals of the

> strategy and include descriptions, responsible organizations, and near-term milestones. (page i)

- DoD Software S&T Strategy (OUSD(R&E) SWSTS 2021): Developed in response to NDAA FY 2020 Section 255, "Department-Wide Software Science and Technology Strategy," this strategy aligns with the DoD Software Modernization Strategy but focuses on the contributions that can be made through R&D and S&T initiatives. (https://www.cto.mil/sea/pg "Software")
- DoD Software S&T I-Plan (OUSD(R&E) 2024) (this document): As a follow-on to the DoD Software S&T Strategy, the I-Plan describes an oversight approach and initial plans to execute the strategy.
- Software S&T Roadmap for Advanced Computing and Software (Roadmap 2024): The roadmap is required by NDAA FY 2021 Section 217 (FY 2021), which assigns responsibility to the Principal Director for each Critical Technology Area for the following:

  > Developing and continuously updating research and technology development roadmaps, funding strategies, and technology transition strategies to ensure (A) the effective and efficient development of new capabilities in the area; and (B) the operational use of appropriate technologies. (Sec. 217 par. (B)(1))

  The Principal Director for Advanced Computing and Software delivered the roadmap in April 2024. The roadmap covers specific areas where S&T is needed to advance the Department's capabilities in software as well as advanced computing infrastructures (e.g., high-end computing, cloud, edge).

2 Oversight Approach

2.1 Governance

The USD(R&E) is responsible for synchronizing S&T efforts across the DoD, the Joint Staff, and the Military Services. The USD(R&E) also has oversight responsibility for critical capabilities managed by Defense Agencies and field activities including the Defense Advanced Research Projects Agency (DARPA), Missile Defense Agency (MDA), and the Defense Innovation Unit (DIU), as well as the Defense Science and Innovation Board offices.

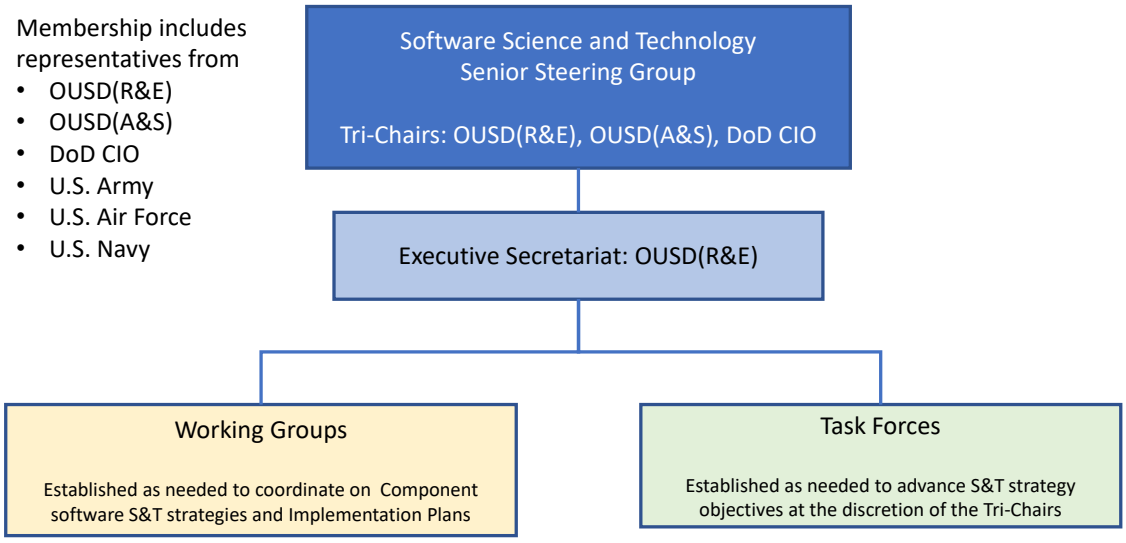

Figure 2-1. DoD Software S&T Strategy Governance

The SW S&T SSG organizes the coordination and resolution of software S&T issues among the DoD Components, Military Services, and Agencies; between DoD and other Federal-level agencies and activities; and with allied and coalition partners, as required. DoD Components consist of the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense.

2.2 Task Planning and Management Approach

2.2.1 Threat-Based Approach to Prioritizing S&T Investment

The Department prioritizes S&T efforts that focus on the joint mission and seeks to invest in information systems and establish processes for rigorous, threat-informed analysis that will better enable the Department to make informed choices in its S&T investments (NDSTS 2023). For purposes of developing this I-Plan, the SW S&T SSG has established the following software S&T priorities:

- Prioritize software S&T investments based on informed analysis of future threats.
- Emphasize moving prototypes into operational assessment with real (classified) operational data quickly. Move first encounter with real data and operators sooner.

- Give weight to balanced coverage of the goals and focus areas enumerated in the 2021 DoD Software S&T Strategy.
- Maintain a balanced portfolio of S&T investments, giving the greatest aggregate potential for success in overcoming the spectrum of potential threats.
- Prevent malware from being surreptitiously inserted into warfighting systems through hardware and software supply chains.
- Engage and collect feedback from acquisition organizations, transition partners, and operational stakeholders to help guide S&T investments.

2.2.2 Potential Threats to National Security Circa 2030

By the year 2030, scientific and technological advances in software threaten to erode U.S. military superiority unless we "continue to deliver disruptive innovations to ensure our nation's defense" (USAF 2019). Failure to innovate could have severe consequences. For example:

- Legacy U.S. weapon systems could be overwhelmed by superior coordination and effectiveness of systems developed and deployed by adversarial nation states targeting our communications, command, control, and intelligence assets.
- Software-dependent warfighting platforms could be rendered ineffective, disabled, or turned against our own forces as result of cyber-attack.
- Adversarial nation-states could deploy breakthrough advances in artificial intelligence (AI) to deploy autonomous weapon systems that operate over air, land, sea, space with orders of magnitude increase in accuracy, speed, and coordination to overwhelm conventionally directed forces.
- Rival nation-states could adapt commercially available software innovations to their own military use, fielding new capability faster and at a scale that the U.S. defense industrial base could not counter in time.
- The United States could fail to align the application of AI in an operational system with the risk tolerance of that system.
    - If overly risk tolerant, naive application of AI/machine learning (ML) technology could result in catastrophic failure when weapon systems are faced with unforeseen circumstances on the battlefield.
    - If overly risk averse, adversary states could field AI-based systems that credibly dominate on the battlefield.
- Cyber attacks on software enabled warfighting systems via supply chains, or exploitable vulnerabilities software or firmware could render them ineffective when needed.
- Ability to deny U.S. military forces access to theater could embolden nation-state adversaries to impose political will on neighbors, harming U.S. interests.

Rather than take a reactive approach to potential threats, our approach is to create innovation while maintaining the foundational S&T institutions, strengthening ties with industry and academia and government research labs. The tasks outlined in Section 3 represent a sampling of key efforts to ensure that the threats enumerated above do not materialize.

3 FY 2024–2025 Goals and Tasks

Table 3-1 summarizes the tasks the SW S&T SSG and Components are tracking to execute the software S&T strategy. The table and the descriptions that follow designate the four goals of the DoD Software S&T Strategy as G1, G2, G3, and G4. Under each goal, subgoals are enumerated at the level "G1.1" I-Plan tasks under each subgoal are enumerated at the level "G1.1.1."

Each task is assigned an Office of Primary Responsibility (OPR) and one or more Office(s) of Coordinating Responsibility (OCR). The table and summaries include an estimated quarter of FY 2024 or FY 2025 in which a milestone delivery occurred or is expected.

A task may simultaneously support multiple strategic goals and multiple focus areas within those goals. The righthand columns indicate milestones for FY 2024 and FY 2025. The tasks here may be traced to the focus areas as detailed in Appendix B.

Two tasks refer to the software factory concept (DSB 2018). While software factories are typically associated with production systems, researchers can adapt the concept to software S&T, reducing barriers to moving from idea to prototype and to delivery.

Research targeting automation of continuous integration/continuous delivery (CI/CD) pipelines as part of a software factory can enable resilient performance at both the strategic and tactical level. Particularly in the context of resilient infrastructure, new methods including AI-enabled orchestration will allow faster recovery for infrastructure in contested environments.

Table 3-1. Summary of Goals and Tasks

ID	Goal/Task	OPR	FY 2024				FY 2025			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
G1	**Goal 1: Shift Engineering and Software Development Left**									
G1.1	Create a research-to-field collaborative technology pipeline									
G1.1.1	Enable DoD-funded research to include potential transition partners as part of the initial research effort	AFSC/SW			✓	♦				
G1.1.2	Integrate DoD-funded research directly into the full platform life cycle	AFSC/SW					♦			
G1.1.3	Embed software workforce professionals with academic institutions to provide education opportunities	AFSC/SW						♦		♦
G1.1.4	Provide mission infrastructure to support continuous operational assessment on classified networks	AFRL/DCO								♦
G1.2	Develop M&S capabilities to guide acquisition and mission decision making									
G1.2.1	Establish a holistic assurance decision-making capability, integrating evidence across the life cycle	OUSD(R&E)								♦
G1.3	Provide a high level of assurance									
G1.3.1	Develop Joint Software Assurance Roadmap to align with the DoD/NNSA Software Assurance Community of Practice (SwA CoP)	OUSD(R&E)				♦				
G1.3.2	Improve assurance through development of supplemental guidance for the integration of DevSecOps and open source software in program protection planning	OUSD(R&E)					♦			
G2	**Goal 2: Adopt an Integrated Framework of Shared Resources**									
G2.1	Make software and supporting data a trusted medium for deploying innovative capabilities									
G2.1.1	Establish assured software repositories	OUSD(R&E)						♦		
G2.1.2	Improve software factory security posture through improved CI/CD pipelines and access to new assurance tools	OUSD(R&E)					♦			
G2.1.3	Enable greater use of data analytics in the DoD S&T community.	OUSD(R&E)				♦		♦		
G2.1.4	Identify potential software S&T activities to advance the DoD Zero Trust Strategy	OUSD(R&E)	✓			♦				
G2.1.5	Implement a federated data fabric that provides ready access to operational data to support development of software capabilities	AFRL								♦
G3	**Goal 3: Transform the Software Workforce**									
G3.1	Train the DoD workforce in automation technologies that accelerate mission attainment									
G3.1.1	Remove barriers to workforce adoption of process automation (e.g., software factories, CI/CD)	OUSD(R&E)	✓							
G3.1.2	Invest in targeted uses of artificial intelligence	OUSD(R&E)				♦				
G3.1.3	Maintain a clearinghouse of hackathons and other software challenges that can help identify talent and improve the state of practice	OUSD(R&E)					♦			♦
G3.2	Enable continuous learning to keep pace with the commercial sector									
G3.2.1	Train the DoD workforce in software S&T advances to accelerate technology transition from research into operations	DAU		✓	✓					
G3.2.2	Provide assurance training available through JFAC portal	OUSD(R&E)							♦	
G3.2.3	Create intermediate and advanced software assurance credentials	DAU				♦				♦
G4	**Goal 4: Align Software S&T with Acquisition**									
G4.1	Develop advanced software capabilities for warfighting teams									
G4.1.1	Ensure DoD is able to access S&T advances to improve software solutions in the Department, and invest in areas where specific advancements are needed	OUSD(R&E)/ AC&S			✓					
G4.1.2	Develop software assurance S&T roadmap and transition plan to assure enterprise capabilities	OUSD(R&E)					♦			
G4.1.3	Deliver prototype of edge computing capabilities to warfighting teams	OUSD(R&E)				♦				
G4.1.4	Inform S&T strategy and roadmap with lessons from rapid delivery of capability under Rapid Defense Experimentation Reserve (RDER)	OUSD(R&E)				♦		♦		♦

G 1 GOAL 1: SHIFT ENGINEERING AND SOFTWARE DEVELOPMENT LEFT

Goal 1 promotes shifting engineering and software development "left" (sooner, faster, earlier in the acquisition life cycle) and aligning S&T initiatives (6.1, 6.2, 6.3) with acquisition programs. It envisions strong collaborative teaming between the Department's research scientists and the engineering community. Connecting S&T with weapon system programs and inserting new technology quickly requires engineering rigor during the ideation phase of RDT&E and shifting development left with the pervasive use of automation. This goal focuses on areas such as: advancing DevSecOps; enhancing resilience through speed; creating and curating high-fidelity hardware-in-the-loop and software-in-the-loop models and simulations; enhancing engineering rigor; ensuring a high level of software assurance; and mitigating technical debt.

G 1.1 Create a research-to-field collaborative technology pipeline.

G 1.1.1 Enable DoD-funded research to include potential transition partners as part of the initial research effort.

OPR: Air Force Sustainment Center Software Directorate (AFSC/SW)
OCR: OUSD(R&E)

The primary way to shift engineering and software development left is by connecting the research community to engineering transition partners. DoD needs a software research transition organization that is capable of teaming engineers with scientists in research organizations for the purpose of actively engaging and designing software-focused research. This collaboration provides the means to transition the research quickly and accurately into a deliverable capability to program offices.

Connecting research and engineering cannot be accomplished only by partnering two organizations that have different areas of expertise. A fundamental shift in organizational processes and investments is needed to ensure success.

Milestones

- AFSC/SW established an Office of Research to identify emerging technologies needed for a supporting program office. (Q3 FY24)
- AFSC/SW work with AFRL to determine the best project in which to collaborate with the intention of transitioning the applied research to a program office. This effort will demonstrate the feasibility of partnering a software organization with a research lab to shift an emerging technology to a delivered capability (Q4 FY24).

G 1.1.2 Integrate DoD-funded research directly into the full platform life cycle.

OPR: AFSC/SW
OCR: OUSD(R&E)

Shifting engineering and software development left requires consolidating newly developed software tools and capabilities from the research community and making them available for reuse. Significant time and resources are wasted re-creating tools and working through contract details related to data rights and IP. DoD would benefit from an established research-focused organization within the DoD's organic software workforce to work with the research community

to identify, develop, transition, and sustain a centralized set of government-controlled capabilities that contract performers are encouraged to use. This consistency could reduce waste and overhead. Such an organization would include an organic software development team dedicated to sustaining and transitioning these technologies to systems.

Milestone

- Form a technology acceleration organization consisting of the established AFSC/SW Office of Research and a supporting software development team. This organization will partner with AFRL to identify a set of pilot tools and begin establishing this research to field a technology transfer pipeline. (Q1 FY25)

G 1.1.3 Embed software workforce professionals with academic institutions to provide educational opportunities.

OPR: AFSC/SW
OCR: OUSD(R&E)

To achieve its goal of transforming the software workforce, the DoD needs to invest in graduate-level educational programs in relevant software S&T fields. Funded graduate-level educational programs for software professionals are necessary to cultivate a workforce that fully understands the advanced technologies being researched and developed in laboratories. The organization investing in these programs will establish a research-focused team that will (1) manage the students obtaining graduate degrees and (2) align the research being conducted for thesis/dissertation topics with the strategic goals of the organization. Upon graduating, the software professional will transfer to a software team to apply the learned expertise to the transition of a research project. The software professional also could be part of the partnering team with a research lab to provide the insight required for a transition.

Milestones

- AFSC/SW develop an educational program designed to send targeted software professionals to academia to obtain graduate degrees in software S&T-related fields. (Q2 FY25)
- AFSC/SW established an Office of Research to coordinate the academic activities with a supporting program office's technology need. Upon completing the education program, a software professional will transfer to a software team to manage technical tasks during transition of a research effort. (Q2 FY25)
- AFSC/SW document experience in implementing this approach and communicate examples in relevant forums and communities of practice so they may serve as a model for other organizations across the DoD enterprise. (Q4 FY25)

G 1.1.4 Provide mission infrastructure to support continuous operational assessment on classified networks

OPR: AFRL Digital Capabilities Office (negotiable)
OCR: AFRL Information Directorate

Shifting software development to the left also means that the software development is exposed to real data and operator feedback early in the development process. Unfortunately, the real data and operators work on classified networks, not on isolated development networks or unclassified

networks. Software development on an unclassified network is running "open loop," which results in significant risks when exposure to real data and operators occurs late in the development cycle. This goal involves creating stepped enclaves, all operating at the end-state classification level, each of which provide an Authority to Operate for the infrastructure with access to other systems restricted according to the residual risks of the software. Most Risk Management Framework controls are provided by the infrastructure, some are waived/accepted because the infrastructure is not for operational use (only assessment of technology), and a few are specific to the software (e.g., scans, STIGed operating system). As more controls are satisfied, software can transition to enclaves with greater access to resources on the operational networks. All along, tools such as remote desktop can permit external operators to peer into the enclave and observe or interact with the software to provide feedback and assessment. Also, because the enclaves are operating at the target classification level, data can be imported through various transfer mechanisms to ensure the software is being developed with realistic or real data.

Milestone

- Demonstrate proof of concept for mission infrastructure support continuous operational assessment (Q4 FY25).

G 1.2 Develop modeling and simulation (M&S) capabilities to guide acquisition and mission decision making.

G 1.2.1 Establish a holistic assurance decision-making capability, integrating evidence across the life cycle

OPR: OUSD(R&E)
OCR: OUSD(A&S), Department of Energy National Nuclear Security Administration (NNSA)

Currently, assurance efforts are often segmented, caused by various drivers: operating domains, system types, organizations, governance, authorities, funding sources, infrastructure segmentation, competency areas, technology, and life cycle processes. Moving forward, trends across the DoD enterprise are toward digital approaches such as commercial cloud adoption, federated data exposure through application programming interfaces, analysis through big data analytics, and better automated support to speed and improve analysis capabilities for better data-informed decision making. To that end, opportunities exist to aggregate data across a federated ecosystem of data repositories containing evidence that support various assurance activities. OUSD(R&E) Joint Federated Assurance Center (JFAC) is seeking to fill this gap using an Assurance Case Framework that can support early identification of assurance risks and mitigations.

Milestone

- Pilot JFAC Automated, Enterprise Scale, Assurance Case Framework. (Q4 FY25)

G 1.3 Provide a high level of assurance.

Software assurance is defined as the level of confidence that software is free of vulnerabilities and will perform as desired. Before software developed as part of any research effort or exploratory prototype can be deployed in the field, it must exhibit the requisite level of justified assurance. Deployment at scale requires the software to be sufficiently reliable, trustworthy,

resilient, and operationally viable. To transition innovation from the research labs to fielded systems at pace, the Department needs to speed development and adoption of technologies, architectures, and engineering practices that speed the process of achieving high levels of assurance.

G 1.3.1 Develop Joint Software Assurance Roadmap to align with the DoD/NNSA Software Assurance Community of Practice (SwA CoP).

OPR: OUSD(R&E)
OCR: NNSA, Department of Homeland Security (DHS) S&T, National Security Agency (NSA)

OUSD(R&E) System Security (SysSec), the NNSA, the NSA Center for Assured Software, and the DHS S&T directorate are establishing a Software Assurance Roadmap. The roadmap will address common challenges across the departments with the goal of reducing duplication of effort and identifying opportunities to inform the Federal R&D Strategy. Execution of the roadmap will be aligned with quarterly meetings of the DoD/NNSA SwA CoP.

Milestone

- Publish Joint Software Assurance Roadmap. (Q4 FY24)

G 1.3.2 Improve assurance through development of supplemental guidance for the integration of DevSecOps and open source software in program protection planning.

OPR: OUSD(R&E)
OCR: NNSA, DHS S&T, NSA

OUSD(R&E) SysSec is updating the Program Protection Plan Outline and Guidance to align with DoD Instruction (DoDI) 5000.87, Program Protection to Maintain Technological Advantage and with DoDI 5000.02, Operation of the Defense Acquisition System. This update will address the adoption of new technologies as part of the DoD Software Modernization Strategy (DoD 2021). To support program use of the guidance, OUSD(R&E) will develop supplemental materials to support program integration of DevSecOps and open source software as part of their program protection activities. Without supplemental guidance, programs run the risk of repeating mistakes in either slowing development unnecessarily or providing inadequate levels of assurance as the Department moves to continuous development and delivery processes for software-enabled capability.

Milestone

- Complete Supplemental Materials for Software Assurance. (Q1 FY25)

G 2 GOAL 2: ADOPT AN INTEGRATED FRAMEWORK OF SHARED RESOURCES

Goal 2 advocates for the use of an integrated framework of shared resources using cloud-native microservices instead of program-specific, monolithic architectures. This goal advocates for research into shared resources to increase collaboration and reuse to prevent redundant, stovepiped development. This goal can be illustrated as the framework of three layers of shared resources. The largest primary layer consists of highly resilient, cloud-native DevSecOps infrastructure environments. The second layer consists of microservices within the federated repositories of programs, models, data, and software. The top layer represents the holistic "value-added" S&T software development environments across the Department. This goal focuses on areas such as: researching highly secure, resilient, cloud-native architectures; leveraging modern ecosystems, technologies, tools, and processes; data acquisition, data science, and event streaming; accelerating delivery and adoption of AI/ML; creating a federated portal for reusable and shared resources; and investing in low-code, no-code, and robotic process automation.

G 2.1 Make software and supporting data a trusted medium for deploying innovative capabilities.

Expanding the adoption of software factory pipelines is key to making software a trusted medium for deploying innovative capabilities. By pooling commonly required capability to perform analysis of software components and systems, and automating repetitive analytical tasks, the Department can increase its ability to deploy trustworthy software at scale with the requisite confidence.

G 2.1.1 Establish assured software repositories.

OPR: OUSD(R&E)
OCR: N/A

To effectively promote software reuse, DoD programs must have confidence that the software functions only as intended and is free of known vulnerabilities. Starting in 2020, JFAC has identified critical software packages that are used across the Department and has piloted efforts to assess, assure, and share the software. Repositories such as the Air Force's Iron Bank provide access to software packages and tools that have already been evaluated to promote reuse. JFAC will continue to enhance these capabilities by establishing an assured software repository that combines the sure reuse capabilities of Iron Bank and the rigorous assessment and mitigation techniques performed by JFAC Service partners throughout the Department.

Milestone

- Pilot assurance software repository capability. (Q2 FY25)

G 2.1.2 Improve software factory security posture through improved continuous integration/continuous delivery (CI/CD) pipelines and access to new assurance tools.

OPR: OUSD(R&E)
OCR: N/A

Public Law 113-66 of the NDAA FY 2014 Section 937 established the JFAC and the requirement for JFAC to enable efficient and affordable acquisition and use of software assurance tools. In 2023, JFAC established an assurance tool catalog to help programs secure their mission system through the selection of commercial off-the-shelf, government off-the-shelf, and open source tools. Through the creation of software factories, the DoD has centralized software development capabilities and tools for DoD systems. This centralization creates a potential for increased software vulnerabilities if secure development practices are not followed. It also creates an opportunity to integrate software assurance tools into CI/CD pipelines that provide software to multiple DoD programs. JFAC will add to the existing assurance tool capabilities and enterprise licensing approach to promote the use of software assurance tools across the DoD's software factory ecosystem.

Milestone

- Provide CI/CD assurance tools for software factory adoption. (Q1 FY25)

G 2.1.3 Enable greater use of data analytics in the DoD S&T community.

OPR: OUSD(R&E)
OCR: CDAO

DoD provides data analytics capabilities that serve to align acquisition with S&T investments; however, limits on their discoverability, availability, and application domain coverage inhibit greater use by the S&T community. Through the AI hubs concept, both operational data and analysis tools could be made available to researchers to develop models and simulations that inform both S&T investments and acquisitions in support of operational need. The models and simulations could help to assess the potential impact of new capabilities in the context of real-world scenarios covering a broad range of potential missions. The operational scenarios and data must cover a broad range of application domains, and the Department will work to extend coverage of those domains both in breadth and depth over time. This task will help ensure that information and tools developed can evolve and transition to the acquisition, test, and training follow-on phases. This task will help ensure that developed S&T capabilities span the valley of death and have operational impact.

Milestones

- SW S&T SSG form a working group to identify repositories of operational data and analysis tools across different application domains and make that information available to both the acquisition and S&T communities. (Q4 FY24)
- Produce recommendations for execution of AI hubs concept to include hosting, execution, and ongoing support. (Q2 FY25)

G 2.1.4 Identify potential software S&T activities to advance the DoD Zero Trust Strategy.

OPR: OUSD(R&E)
OCR: DoD CIO

The DoD CIO is developing a Zero Trust (ZT) strategy to move beyond traditional network security methods to modern approaches more suited to mobile computing, cloud services, and flexible or intermittent connectivity that enable reliable distributed systems in the face of cyber and physical threats in contested environments. Operators at the tactical edge should not have their operations degraded by loss of cloud connectivity. OUSD(R&E) will collaborate with DoD CIO to identify specific steps that the Department can take to encourage software S&T research to both leverage the ZT framework and contribute research to improve the state of the art of its supporting technology and practice.

Milestones

- Delivered the Zero Trust Strategy by DoD CIO. (Q1 FY24)
- Identify opportunities to support software S&T activities with ZT-based connectivity to enterprise resources. (Q4 FY24)

G 2.1.5 Implement a federated data fabric that provides ready access to operational data to support development of software capabilities.

OPR: OUSD(R&E)
OCR: AFRL Information Directorate

Implement a data fabric to provide mediated access to data to support software development, and ultimately operation. The most challenging element of this goal is not the technologies for data sharing but managing the data-sharing agreements among the large and diverse set of data providers and their consumers. Data may be provided with differing levels of assurance (availability) or only for certain classes of use cases (suitability). These agreements often take the form of Memorandums of Understanding, Memorandums of Agreement, or Data Exchange agreements, not programming interfaces; however, once the agreements are in place, technologies are available to enforce the terms of those agreements and provide access to software developers.

Milestone

- Develop model information-sharing agreements. (Q4 FY25)

G 3 GOAL 3: TRANSFORM THE SOFTWARE WORKFORCE

Goal 3 promotes a cultural transformation to better connect research scientists with the software engineering workforce. It reflects DoD's responsibility to create overmatching software capabilities and to build a digital cyber-talented workforce. This goal accelerates the use of new technologies to enhance the identification, recruitment, retention, and development of a superior S&T and software engineering workforce. It states the DoD must compete to hire, train, and retain software engineers, platform engineers, AI/ML engineers, data scientists, and research scientists, as the commercial sector is acquiring this talent much faster than the Government. DoD must hire and train core software personnel to manage the DevSecOps tech stack and "undifferentiated heavy lifting" so research scientists can focus on innovation, advancing the technology, algorithm, and code development. This goal focuses on areas such as: connecting the S&T and engineering workforce; training and investing in data science, AI/ML, and software engineering; cultivating a leading S&T and software engineering workforce; enabling continuous learning to keep pace with the commercial sector; and elastically scaling the software development workforce.

G 3.1 Train the DoD workforce in automation technologies that accelerate mission attainment

G 3.1.1 Remove barriers to workforce adoption of process automation (e.g., software factories, CI/CD).

OPR: OUSD(R&E)
OCR: N/A

In the past, system administrators manually configured computer hardware, installing operating systems and configuring applications, networks, and routers. Test engineers would write up test plans and manually carry out test procedures that took hours or days, requiring a large team of testers. In modern organizations, these manual tasks are now carried out by automated tools in a software factory framework. Testing makes extensive use of test scripts, test script generators, and software analysis tools for a more highly automated process. There is a change, not just in the technology, but in the work roles and capabilities of the workforce required for organizations to execute these automated processes.

Milestone

- Completed codification of software engineering work roles available to software development teams that employ software factories, infrastructure as code, and CI/CD pipelines. Officially recognized work role definitions help remove administrative obstacles and facilitate recruitment, training, development, and retention of a modern DoD workforce. (Q1 FY24)

G 3.1.2 Invest in targeted uses of artificial intelligence.

OPR: OUSD(R&E)
OCR: N/A

Advances in AI have captured much attention in recent years. Commercial applications of AI are finding broad acceptance in speech and image recognition and natural language processes.

Generative AI has shown impressive results in image generation and the natural language interactions with human users. The potential application to warfighting and intelligence analysis is undeniable, but so too is their potential misapplication. Prototyping is needed to understand and characterize what applications make a good fit for what AI technologies.

Milestone

- Identify prototyping efforts in targeted uses of artificial intelligence. (Q4 FY24)

G 3.1.3 Maintain a clearinghouse of hackathons and other software challenges that can help identify talent and improve the state of practice.

OPR: OUSD(R&E)
OCR: N/A

Hackathons and other software competitions have always been important forums for understanding representative challenges and the state of the art in addressing them. Potential competitors would benefit from being able to find out about opportunities more easily, and organizations across the Department would benefit from sharing lessons learned and understanding how well competitors perform.

An example of the type of event would be the following (DARPA AIxCC 2023):

> DARPA Cyber Challenge (AIxCC) – a 2-year competition aimed at driving innovation at the nexus of AI and cybersecurity to create a new generation of cybersecurity tools. AIxCC brings together leading AI companies to make their cutting-edge technology and expertise available to challenge competitors. Anthropic, Google, Microsoft, and OpenAI will collaborate with DARPA to enable competitors to develop state-of-the-art cybersecurity systems. The Open Source Security Foundation (OpenSSF), a project of the Linux Foundation, will serve as a challenge advisor to guide teams in creating AI systems capable of addressing vital cybersecurity issues, such as the security of our critical infrastructure and software supply chains. Most software, and thus most of the code needing protection, is open-source software, often developed by community-driven volunteers. AIxCC competitions will be held at DEF CON with additional events at Black Hat USA, both of which are internationally recognized cybersecurity conferences that draw tens of thousands of experts, practitioners, and spectators from around the world to Las Vegas every August. AIxCC will consist of two phases: the semifinal phase and the final phase. The semifinal competition and the final competition will be held at DEF CON in Las Vegas in 2024 and 2025. (DARPA AIxCC 2023)

Milestones

- Stand up team; hold kickoff. (Q1 FY25)
- Publish MVP list / clearinghouse. (Q4 FY25)

G 3.2 Enable continuous learning to keep pace with the commercial sector.

G 3.2.1 Train the DoD workforce in software S&T advances to accelerate technology transition from research into operations.

OPR: Defense Acquisition University (DAU)
OCR: OUSD(R&E)

DAU is preparing the workforce to transition new software capabilities into operation. Through a combination of custom-developed and commercially available courses and micro-learning assets, members of the DoD workforce received training in AI foundations, fundamental secure cyber-resilient engineering, DevSecOps practices and tools, and more.

Milestones

- Deployed Artificial Intelligence Foundations in DoD Credential. (Q2 FY24)
- Deployed 88 of 158 Learning Assets for DevSecOps Intermediate Credential Series. (Q3 FY24)
- Deployed 4 of 5 Learning Assets for Fundamental Secure Cyber-Resilient Engineering Credential. (Q3 FY24)

G 3.2.2 Provide assurance training available through JFAC portal.

OPR: OUSD(R&E)
OCR: N/A

The JFAC provides a federation of software and hardware assurance capabilities across the DoD with the vision of building trust through holistic assurance. Currently the JFAC offers assurance capabilities and resources including the trust and assurance knowledge management, assurance tool catalog, and federated assurance ecosystem. In 2024, JFAC will expand existing capabilities to include a collection of assurance training, providing the DoD workforce with access to DoD and commercial training products. https://jfac.dso.mil

Milestone

- Deploy JFAC Training Catalog. (Q3 FY25)

G 3.2.3 Create intermediate and advanced software assurance credentials.

OPR: DAU
OCR: OUSD(R&E)

The DAU Engineering and Technical Management functional area has identified nine software assurance credentials, including intermediate and advanced software assurance credentials. Most computer science and engineering curriculums do not include secure software architecture or development practices. The DAU software assurance credentials will provide students with an understanding of secure architecture, development, supply chain, and software assurance analysis techniques required to protect mission-critical functions and components. OUSD(R&E) and SwA CoP will provide subject matter expertise to guide DAU content development.

Milestones

- Intermediate Credential September 2024. (Q4 FY24)
- Advanced Credential September 2025. (Q4 FY25)

G 4 GOAL 4: ALIGN SOFTWARE S&T WITH ACQUISITION

Goal 4 seeks to align software S&T efforts with DoD acquisition. The United States possesses the best-equipped military in the world. Sustaining technical superiority over our adversaries requires an acquisition system in which innovative technology can be rapidly integrated into warfighting systems. The DoD acquisition system must be flexible, confront the transition risk, and bridge the "valley of death" from concept exploration to acquisition. Use of the Software Acquisition Pathway policy (USD(A&S) 2020) will help mitigate many of the acquisition challenges affecting schedules; it was built to support rapid technology innovation and alignment with commercial approaches. This goal focuses on areas such as bridging the gap between S&T and acquisition; embracing the mind-set that software is never done; advocating a strategic outlook toward S&T investments; investing in leap-forward technology to leverage industry best practices; and streamlining the planning, funding, requirements, and contracting process.

G 4.1 Develop advanced software capabilities for warfighting teams.

G 4.1.1 Ensure DoD can access S&T advances to improve software solutions in the Department, and invest in areas where specific advancements are needed.

OPR: OUSD(R&E)/Principal Director for Advanced Computing and Software (AC&S)
OCR: N/A

A central theme for DoD software S&T is that "software is never done": Technologies, end user expectations, and dynamic mission needs all change so rapidly that there is almost always a demand for more and better software-enabled capabilities in DoD systems. Similarly, DoD software and computing infrastructure needs to be able to evolve constantly. DoD must be open to engineering advances in software and computing, taking advantage of them appropriately to continuously improve the way we develop and deploy DoD capabilities, implementing a "fast follower" strategy. As required by Congress (NDAA 2021 Sec 217), the Principal Director for AC&S is constructing an S&T roadmap that will articulate major areas of S&T focus for the Department and how the areas align with software modernization needs.

Software is ubiquitous in the Department, and as a result, the S&T roadmap is being developed through engagements with multiple stakeholders: Service leadership, Program Executive Officers (PEOs), and program managers, which have ambitious acquisition and mission needs; the S&T community, which is making strategic investments in advanced technologies; the Department's software factories and enterprise platforms, which are likely to be important transition partners; and many others. The Principal Director for AC&S is building an unclassified version of the roadmap to ensure the Department can engage effectively with industry and academia to glean insights and understand work that can contribute to addressing Departmental needs. Important areas of work being explored for the AC&S roadmap include:

- SW Engineering: New technologies implemented in software (like AI/ML), mission needs, and evolving threats create new challenges for the engineering of complex systems that are interoperable, safe, secure, adaptable, resilient, and capable.
- SW Acquisition: The DoD acquisition ecosystem needs to be supported in its ongoing transformation to deliver capabilities at a faster cadence, to outpace adversaries.

- Computing Architectures: The DoD's future operating concepts and need for high-fidelity modeling and decision support require continued advancement in specialized computing architectures, e.g., supercomputing, edge, cloud.
- Workforce Effectiveness: The DoD has unique software requirements that need skilled (and cleared) experts able to write new code and translate legacy code but has trouble competing with industry for important skill sets. Tools and automation can improve the productivity of our current workforce and improve the way we track expertise.
- Mission Capability Integration: For DoD systems to provide warfighter advantage over near/peer adversaries, advances are required in important application areas (e.g., computer vision, data fusion, and decision support).

Modern software development methodologies such as agile, DevSecOps, and continuous delivery all stress user engagement and rapid delivery, putting a product in the hands of the user to surface needs, set priorities, and direct effort to produce the highest value to the stakeholders. Newer variants such as low-code, no-code take this a step further by developing flexible self-service products that users with little or no programming experience can tailor to their need. Advantages include (1) making efficient use of scarce programming talent; (2) less opportunity to introduce security vulnerabilities; and (3) improved capability to leverage the domain expertise of the user to rapidly address emergent needs.

Milestone

- Completed the S&T Roadmap: (1) identified existing DoD S&T investments in these topics; (2) identified complementary research (academic and commercial) from other sources, which can provide capabilities to be adapted by the Department as part of its "fast follower" strategy in this area; and (3) developed a vision of near-, mid-, and long-term DoD needs in this area to identify gaps and articulate commercial products and external research that would be of interest to DoD. (Q3 FY24)

G 4.1.2 Develop software assurance S&T roadmap and transition plan to assure enterprise capabilities.

OPR: OUSD(R&E)
OCR: N/A

In accordance with NDAA FY 2014 Section 937, JFAC is responsible for ensuring that requirements to innovate software vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development. JFAC is developing a JFAC Assurance S&T Roadmap to include discovery and identification of enterprise assurance gaps/needs, S&T investments across the DoD, and awareness of commercially available assurance solutions.

Milestone

- Deliver Software Assurance S&T Roadmap. (Q1 FY25)

G 4.1.3 Deliver prototype of edge computing capabilities to warfighting teams.

OPR: OUSD(R&E)
OCR: N/A

Edge computing brings computation and data storage closer to the location where it is needed, improving response times and saving communications bandwidth. In contrast, many legacy systems send sensor data collected on the battlefield across global networks to be processed on the other side of the world before providing critical information back to the warfighter. Technologies contributing to edge computing include mesh networks, micro data centers, cloud of things, 5G and WiFi-6 technology, augmented reality, and virtual reality. DoD is prototyping these capabilities to enhance the effectiveness of warfighting teams.

Milestone

- Identify best of breed research in edge computing S&T prototyping efforts and facilitate their inclusion in military exercises. (Q4 FY24)

G 4.1.4 Inform S&T strategy and roadmap with lessons from rapid delivery of capability under Rapid Defense Experimentation Reserve (RDER).

OPR: OUSD(R&E)
OCR: N/A

The RDER is a collaboration among the Military Services, Combatant Commands, industry, and coalition partners to quickly get promising technology and prototypes into the hands of U.S. warfighters. These experiments are critical for understanding effective methods for moving advanced technologies to the warfighter speedily and effectively. While the RDER experiments are concerned about mission capabilities rather than software per se, many of them are expected to include important software-enabled capabilities.

Milestones

- Analyze which RDER experiments include software capabilities as an important part of the warfighter capability being fielded. (Q4 FY24)
- Survey of RDER experiments to identify: (Q2 FY25)
    - Enablers/best practices that contributed to quick adaptation and fielding of software capabilities. These may lead to areas of work for the S&T strategy, to ensure those best practices can be replicated at scale by other efforts in the Department.
    - Obstacles/areas where future work is needed, which may inform the needed capabilities addressed by the S&T Roadmap.
- Explore whether there is a need for a new RDER proposal to address needed capabilities called out in the S&T Strategy. (Q4 FY25)

Appendix A: I-Plan Tasks Mapped to Software S&T Strategy Focus Areas

Table A-1 maps the focus areas in the DoD Software S&T Strategy (2021) to the tasks specified in this I-Plan.

Table A-1. Software S&T Focus Areas Mapped to I-Plan Tasks

Focus Area	Focus Areas specified in Software S&T Strategy (2021)
Goal 1	Goal 1: Shift Engineering and Software Development Left
FA2.1.1	Advance DevSecOps (DSO)
FA2.1.2	Enhance Resilience Through Speed
FA2.1.3	Create and Curate SWIL & HWIL Modeling & Simulation (M&S)
FA2.1.4	Enhance Engineering Rigor
FA2.1.5	Ensure a High Level of Software Assurance
FA2.1.6	Mitigate Technical Debt
Goal 2	Goal 2: Adopt an Integrated Framework of Shared Resources
FA2.2.1	Research Highly Secure, Resilient, Cloud-Native Architectures
FA2.2.2	Leverage Modern Ecosystems, Technologies, Tools, and Processes
FA2.2.3	Focus on Data Acquisition, Data Science, and Event Streaming
FA2.2.4	Accelerate Delivery and Adoption of AI/ML
FA2.2.5	Create Federated Portal for Reusable and Shared Resources
FA2.2.6	Invest in Low-Code, No-Code, and Robotic Process Automation (RPA)
Goal 3	Goal 3: Transform the Software Workforce
FA2.3.1	Connect the S&T and Engineering Workforce
FA2.3.2	Train and Invest in Data Science, AI/ML, and Software Engineering
FA2.3.3	Cultivate a Leading S&T and Software Engineering Workforce
FA2.3.4	Enable Continuous Learning to Keep Pace with the Commercial Sector
FA2.3.5	Elastically Scale the Software Development Workforce
Goal 4	Goal 4: Align Software S&T with Acquisition
FA2.4.1	Bridge the Gap Between S&T and Acquisition
FA2.4.2	Embrace the Mind-set that Software Is Never Done
FA2.4.3	Advocate a Strategic Outlook toward S&T Investments
FA2.4.4	Invest in Leap-Forward Tech to Leverage Industry Best Practices
FA2.4.5	Streamline the Planning, Funding, Requirements, and Contracting Process
Task	**Tasks Specified in Software S&T I-Plan (2024)**
Goal 1	Goal 1: Shift Engineering and Software Development Left
G1.1.1	Enable DoD-funded research to include potential transition...
G1.1.2	Integrate DoD funded research directly into the full platform...
G1.1.3	Embed software workforce professionals with academic insititutions..
G1.1.4	Provide mission infrastructure to support cointinuous ...
G1.2.1	Establish a holistic assurance decision making capability ...
G1.3.1	Develop Joint Software Assurance Roadmap to align with ...
G1.3.2	Improve assurance through development of supplemental ...
Goal 2	Goal 2: Adopt an Integrated Framework of Shared Resources
G2.1.1	Establish assured software repositories
G2.1.2	Improve software factory security posture through improved CI/CD
G2.1.3	Enable greater use of data analytics in the DoD S&T community
G2.1.4	Identify potential software S&T activities to advance the DoD Zero...
G2.1.5	Implement a data fabric to provide mediated access to data ...
Goal 3	Transform the Software Workforce
G3.1.1	Remove barriers to workforce adoption of process automation
G3.1.2	Invest in targeted uses of artificial intelligence
G3.1.3	Maintain a clearing house of hackathons and other software ....
G3.2.1	Train the DoD workforce in software S&T advances to accelerate...
G3.2.2	Provide assurance training available through JFAC portal
G3.2.3	Create intermediate and advance software assurance credentials
Goal 4	Goal 4: Align Software S&T with Acquisition
G4.1.1	Ensure DoD is able to access S&T advances to improve software...
G4.1.2	Software assurance S&T roadmap and transition plan to ensure...
G4.1.3	Prototype delivery of edge computing capabilities to warfighting...
G4.1.4	Inform S&T strategy and roadmap with lessons from rapid delivery

The row labels in the top section each begin with “FA” and map to section numbers in the Software S&T Strategy that specify a focus area. For example, “FA2.1.1” refers to section 2.1.1 of the Strategy, which defines the focus area “Advance DevSecOps.”

The row labels in the bottom section each begin with “G” and refer to tasks specified in this I-Plan. For example, “G.1.1.1” refers to “Enable DoD-funded research to include potential transition partners as part of the initial research effort” specified in page 8 of this I-Plan.

The dark boxes in the bottom right corner indicate the top two to four focus areas deemed by the authors to be those most closely associated with each task.

Appendix B: NDAA FY 2020 Section 255

SEC. 255. DEPARTMENT-WIDE SOFTWARE SCIENCE AND TECHNOLOGY STRATEGY.

(a) DESIGNATION OF SENIOR OFFICIAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering and in consultation with the Under Secretary of Defense for Acquisition and Sustainment and appropriate public and private sector organizations, shall designate a single official or existing entity within the Department of Defense as the official or entity (as the case may be) with principal responsibility for guiding the development of science and technology activities related to next generation software and software reliant systems for the Department, including—

(1) research and development activities on new technologies for the creation of highly secure, scalable, reliable, time-sensitive, and mission-critical software;

(2) research and development activities on new approaches and tools to software development and deployment, testing, integration, and next generation software management tools to support the rapid insertion of such software into defense systems;

(3) foundational scientific research activities to support advances in software;

(4) technical workforce and infrastructure to support defense science and technology and software needs and mission requirements;

(5) providing capabilities, including technologies, systems, and technical expertise to support improved acquisition of software reliant business and warfighting systems; and

(6) providing capabilities, including technologies, systems, and technical expertise to support defense operational missions which are reliant on software.

(b) DEVELOPMENT OF STRATEGY. — The official or entity designated under subsection (a) shall develop a Department-wide strategy for the research and development of next generation software and software reliant systems for the Department of Defense, including strategies for—

(1) types of software-related activities within the science and technology portfolio of the Department;

(2) investment in new approaches to software development and deployment, and next generation management tools;

(3) ongoing research and other support of academic, commercial, and development community efforts to innovate the software development, engineering, and testing process, automated testing, assurance and certification for safety and mission critical systems, large scale deployment, and sustainment;

(4) to the extent practicable, implementing or continuing the implementation of the recommendations set forth in—

(A) the final report of the Defense Innovation Board submitted to the congressional defense committees under section 872 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1497);

(B) the final report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems described in section 868 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2223 note); and

(C) other relevant studies on software research, development, and acquisition activities of the Department of Defense.

(5) supporting the acquisition, technology development, testing, assurance, and certification and operational needs of the Department through the development of capabilities, including personnel and research and production infrastructure, and programs in—

(A) the science and technology reinvention laboratories (as designated under section 1105 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 10 U.S.C. 2358 note));

(B) the facilities of the Major Range and Test Facility Base (as defined in section 2358a(f)(3) of title 10, United States Code);

(C) the Defense Advanced Research Projects Agency; and

(D) universities, federally funded research and development centers, and service organizations with activities in software engineering; and

(6) the transition of relevant capabilities and technologies to relevant programs of the Department, including software-reliant cyber-physical systems, tactical systems, enterprise systems, and business systems.

(c) SUBMITTAL TO CONGRESS. —Not later than one year after the date of the enactment of this Act, the official or entity designated under subsection (a) shall submit to the congressional defense committees the strategy developed under subsection (b).

Glossary

Continuous Integration/Continuous Delivery (CI/CD) Pipeline: The set of tools and the associated process workflows to achieve continuous integration and continuous delivery with build, test, security, and release delivery activities, which are steered by a CI/CD orchestrator and automated as much as practice allows. (DoD CIO 2019)

DevSecOps: 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 life cycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted left through automated unit, functional, integration, and security testing. This shift differentiates DevSecOps from other methods of software development in that security and functional capabilities are tested and built simultaneously.

Software Engineering (SWE): (1) The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software. (2) The study of approaches as in (1). (Source: IEEE Standard Glossary of Software Engineering Terminology. Washington, DC: Institute of Electronical and Electronics Engineers. IEEE 610.12-1990; Systems Engineering Body of Knowledge Wiki https://sebokwiki.org/wiki/Software_Engineering_(glossary))

Software Factory: A software assembly plant that contains multiple pipelines, which are 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. The software factory supports multitenancy. (DoD CIO 2019)

Acronyms

AC&S	Advanced Computing and Software
AI/ML	Artificial Intelligence/Machine Learning
AIxCC	AI Cyber Challenge
AFSC/SW	Air Force Sustainment Center Software Directorate
CI/CD	Continuous Integration/Continuous Delivery
DARPA	Defense Advanced Research Projects Administration
DAU	Defense Acquisition University
DHS	Department of Homeland Security
JFAC	Joint Federated Assurance Center
M&S	Modeling and Simulation
NDAA	National Defense Authorization Act
NNSA	National Nuclear Security Administration
NSA	National Security Agency
OpenSSF	Open Source Security Foundation
OCR	Office of Collateral Responsibility
OPR	Office of Primary Responsibility
OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
OUSD(R&E) SysSec	OUSD(R&E) System Security
RDER	Rapid Defense Experimentation Reserve
RDT&E	Research, Development, Test, and Evaluation
SW S&T SSG	Software Science and Technology Strategy Senior Steering Group
SSG	Senior Steering Group
S&T	Science and Technology
SwA	Software Assurance
SWE	Software Engineering

References

DARPA AIxCC. 2023. *Defense Advanced Research Projects Agency (DARPA) Artificial Intelligence (AI) Cyber Challenge (AIxCC).* Accessed July 2024. https://aicyberchallenge.com.

Defense Science Board (DSB). 2018. *Design and Acquisition of Software for Defense Systems.* OUSD(R&E). https://dsb.cto.mil/wp-content/uploads/dsb/site/wwwroot/reports/2010s/DSB_SWA_Report_FINALdelivered2-21-2018.pdf.

DoD CIO. 2023. *Department of Defense (DoD) Software Modernization Implementation Plan.* DoD Chief Information Officer (CIO). https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-PlanExecutiveSummary.pdf.

DoD CIO. 2019. *DoD Enterprise DefSecOps Reference Design, Version 1.0.* DoD Chief Information Officer (CIO). https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf.

DoD. 2021. *DoD Software Modernization Strategy, Version 1.0.* Washington, D.C.: Department of Defense (November). https://media.defense.gov/2022/Feb/03/2002932833/-1/-1/1/DEPARTMENT-OF-DEFENSE-SOFTWARE-MODERNIZATION-STRATEGY.PDF.

DoD. 2017. "Financial Management Regulation." https://comptroller.defense.gov/portals/45/documents/fmr/current/02b/02b_05.pdf.

Lack, Michael. 2023. "Resilient Anonymous Communication for Everyone (RACE)." *Defense Advanced Research Projects Agency (DARPA).* Accessed February 29, 2024. https://www.darpa.mil/program/resilient-anonymous-communication-for-everyone.

National Intelligence Council. 2021. *Global Trends.* Office of the Director of National Intelligence. https://www.dni.gov/index.php/global-trends-home.

NDAA. FY 2021. "National Defense Authorization Act (NDAA) 2021 Section 217." https://www.acq.osd.mil/dpap/dars/docs/early_engagement_opportunity/HR_6395-116_Enrolled_FY21_NDAA.pdf.

NDAA. FY 2020. *National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020. P.L. 116-92, Section 255: "Department-Wide Software Science and Technology Strategy." December 29, 2019.* Washington, D.C.: 116th Congress.

NDAA. FY 2014. "Public Law 113-66 National Defense Authorizatoin Act for Fiscal Year 2014." https://www.govinfo.gov/content/pkg/PLAW-113publ66/pdf/PLAW-113publ66.pdf.

NDS Fact Sheet. 2022. *Summary of the 2022 National Defense Strategy.* Washington, D.C.: Secretary of Defense.

NDSTS. 2023. *National Defense Science and Technology Strategy (NDSTS).* Department of Defense (DoD). https://www.cto.mil/ndsts/.

OUSD(R&E). 2024. *Science and Technology (S&T) Roadmap for Advanced Computing and Software.* Department of Defense. https://www.dodtechipedia.mil/dodwiki/pages/viewpage.action?pageId=814187236.

OUSD(R&E) SWSTS. 2021. *DoD Software Science and Technology Strategy [SWSTS].* Washington, D.C.: Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). https://www.cto.mil/wp-content/uploads/2023/07/DoD-Software-ST-Strat-2021.pdf.

Schurgot, Mary R. 2023. "Mission-Integrated Network Control (MINC)." *Defense Advanced Research Projects Agency.* Accessed February 29, 2024. https://www.darpa.mil/program/mission-integrated-network-control.

USAF. 2019. "Air Force Science and Technology Strategy." April.

USD(A&S). 2020. *Software Acquisition Pathway Interim Policy and Procedures.* Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)).

This page is intentionally blank.

DoD Software Science and Technology Strategy Implementation Plan
August 2024

Office of Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301
osd-sea@mail.mil
https://www.cto.mil/sea/