Department of Defense Software Science and Technology Strategy

In response to National Defense Authorization Act for Fiscal Year 2020 (P.L. 116-92) Section 255

November 2021

Department of Defense (DoD) Software Strategy Coordinator

Office of the Under Secretary of Defense
for Research and Engineering

Washington, D.C.

The estimated cost of this report or study for the Department of Defense is approximately $159,000 in Fiscal Years 2020 - 2021. This includes $125,000 in expenses and $34,000 in DoD labor.

Generated on 2021May20 RefID: E-2732D97

Department of Defense Software Science and Technology Strategy

Department of Defense (DoD) Software Strategy Coordinator
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301

Contents

Figures

Tables

Executive Summary

In response to the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 (P.L. 116-92) Section 255, the Under Secretary of Defense for Research and Engineering (USD(R&E)) designated the position of Department of Defense (DoD) Software Strategy Coordinator (DSSC) to lead activities and develop a strategy for delivering next-generation DoD software and software-reliant systems. This document describes the DSSC's strategy, which will undergo ongoing review to keep pace with changes in technology and DoD advances.

To develop this strategy, the DSSC consulted with software subject matter experts (SMEs) in the offices of the USD for Acquisition and Sustainment (A&S), the DoD Chief Information Officer (CIO), the Director of Operational Test and Evaluation (DOT&E), Army, Navy, Air Force, and Federally Funded Research and Development Centers (FFRDCs).

The DSSC strategic vision is to *Deliver resilient software capabilities at the speed of relevance*. The DSSC developed four strategic goals to support this vision:

Goal 1: Shift engineering and software development left.

Goal 2: Adopt an integrated framework of shared resources.

Goal 3: Transform the software workforce.

Goal 4: Align software science and technology with acquisition.

Table 1 summarizes the strategy's vision, goals, and focus areas.

Table 1. Software S&T Strategic Vision, Goals, and Focus Areas

	STRATEGIC VISION - DELIVER RESILIENT SOFTWARE CAPABILITIES AT THE SPEED OF RELEVANCE			
Goals	**2.1 SHIFT ENGINEERING AND DEVELOPMENT LEFT**	**2.2 ADOPT AN INTEGRATED FRAMEWORK OF SHARED RESOURCES**	**2.3 TRANSFORM THE SOFTWARE WORKFORCE**	**2.4 ALIGN SOFTWARE S&T WITH ACQUISITION**
Focus Areas	• Advance DevSecOps • Enhance resilience through speed • Create and curate high fidelity HWIL/SWIL, and M&S • Enhance engineering rigor and employ pervasive automation and self-service • Ensure a high level of assurance • Mitigate technical debt	• Research highly secure, resilient, cloud-native architectures • Leverage modern ecosystems, technologies, tools and processes • Focus on data acquisition, data science and event streaming • Accelerate delivery and adoption of AI/ML • Create federated repositories of reusable and shared resources • Invest in low-code, no-code and robotic process automation	• Connect the S&T and Engineering workforce • Train and invest in data science, AI/ML, and software engineering • Cultivate a leading S&T and software engineering workforce • Enable continuous learning to keep pace with the commercial sector • Elastically scale the software development workforce	• Bridge the gap between S&T and Acquisition • Embrace the mindset that software is never done • Advocate a strategic outlook toward software S&T investments • Invest in leap forward tech to leverage industry best practices • Streamline the planning, funding, requirements, and contracting process
NDAA Sec(b)	FY2020 NDAA Section 255 (b) 1 to 6. Including Strategies for: 3.1 Types of Software Related Activities within the Science and Technology Portfolio of the Department 3.2 Investment in New Approaches to Software Development, Deployment, and Next Generation Management Tools 3.3 Research to Innovate the Software Development Engineering, and Testing Process for Safety and Mission Critical Systems 3.4 Status of Implementing Recommendations on Software 3.5 Supporting the Acquisition, Technology Development, Testing, Assurance, and Certification 3.6 The Transition of Relevant Capabilities and Technologies to Programs			

The focus areas are intended to advance and enable the rapid transition of software-developed capabilities to acquisition programs of record through research and development (R&D) and science and technology (S&T) initiatives. In addition to describing the focus areas, this report includes an overview of complementary strategies among DoD Components and the status of related Defense Science Board and Defense Innovation Board recommendations.[1] [2]

DoD S&T software activities address a variety of disparate software needs, including high-performance algorithms, human systems integration, domain-specific systems, and embedded systems supporting cyber-physical platforms, including weapons, sensors, and more. The Department will need to advance the adoption of modern commercial tool sets; cloud-native systems; edge computing; reusable enterprise software; highly resilient, reliable, and high-performance message buses; military Internet of Things; ubiquitous connectivity; and other novel capabilities.

The vision, goals, and focus areas constitute the DoD strategy guiding the development of S&T activities for next-generation software and software-reliant systems. The DSSC will continue to work with collaborators in the defense community to implement the strategy and pursue software S&T advances in basic research, applied research, and advanced technology development.

[1] *Department of Defense Design and Acquisition of Software for Defense Systems.* Office of the Under Secretary of Defense for Research and Engineering, Washington, D.C., February 2018. https://dsb.cto.mil/reports/2010s/DSB_SWA_Report_FINALdelivered2-21-2018.pdf

[2] *Report of the Defense Science Board Task Force on Defense Software.* Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C., November 2000. https://dsb.cto.mil/reports/2000s/ADA385923.pdf

1 Introduction

The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 (P.L. 116-92) Section 255 directed the Secretary of Defense, through the Under Secretary of Defense for Research and Engineering (USD(R&E)), to designate an individual or entity "with principal responsibility for guiding the development of science and technology [S&T] activities related to next-generation software and software-reliant systems." The Act further directed that the designated official develops a Department-wide strategy for the research and development (R&D) of next generation-software and software-reliant systems for the Department of Defense (DoD).

The USD(R&E) designated the position of DoD Software S&T Coordinator (DSSC) to lead the development of this strategy. The DSSC consulted with software experts from across the Department, interagency, industry, and academia to arrive at a vision and goals to advance DoD software engineering. The DSSC and Communities of Interest (COIs) will continue to review the strategy to keep pace with changes in technology and the Department's advances.

Winning a future fight depends on the U.S. ability to deliver fully integrated software-based capabilities faster than its adversaries. Rivals are acquiring military capabilities, especially digital capabilities, at a pace that challenges U.S. technological superiority. The Office of the Director of National Intelligence[3] latest assessment of key global trends describes a changing geopolitical environment and imbalance in global wealth and resources, driving unprecedented social, economic, political, and security challenges. Given global unrest, rapid deployment of software capabilities to support the warfighter is more important than ever before. This strategy supports DoD ability to respond rapidly.

Weapon systems incorporate all aspects of commercial technology including 5G, cyber, autonomous vehicles, Military Internet of Things (MIoT), and artificial intelligence/machine learning (AI/ML). Corporations in the United States and other nation states are making bold moves to dominate the AI economy, investing billions of dollars in data collection, data warehousing, and AI talent. Principal among global competitors is China,[4] [5] whose stated goal is to dominate and become a world leader in AI by 2030. As economist, Indermit Gill[6] wrote in January 2020, *"whoever leads in artificial intelligence in 2030 will rule the world until 2100."* The United States must lead, not only in AI, but in software, as software is the foundation and building material for AI.

To compete in this context, DoD must advance and accelerate the secure delivery of new software capabilities into weapon systems. In this strategy, the DSSC describes a vision and four strategic goals, with supporting focus areas, to enable software-developed capabilities to make

[3] *Global Trends.* National Intelligence Council, 2017. https://www.dni.gov/index.php/global-trends-home
[4] "Will China Lead the World in AI by 2030?" Sarah O'Meara, *Nature,* August 21, 2019. https://www.nature.com/articles/d41586-019-02360-7
[5] "AI Policy – China." Future of Life Institute, February 2020. https://futureoflife.org/ai-policy-china/
[6] "Whoever Leads in Artificial Intelligence in 2030 Will Rule the World until 2100." Indermit Gill, Brookings Institution, Washington, D.C.: January 17, 2020.

the transition from R&D and S&T[7] initiatives to acquisition programs of record. This document is intended to guide strategic thinking within the Department with regard to modern software development approaches and connecting the innovative capabilities developed from S&T investments. The strategy is intended to be thought provoking and to enable a culture focused on modern software development processes and tools on par with the commercial sector, which the Department can leverage to insert new and innovating software capabilities quickly into DoD weapon systems.

[7] Includes programs consisting of Basic Research, Applied Research, and Advanced Technology Development, which are identified as Budget Activities 1, 2, and 3, respectively, in DoD 7000.14R.

2 Vision: Deliver Resilient Software Capabilities at the Speed of Relevance

The DSSC strategic vision for S&T software is to *Deliver resilient software capabilities at the speed of relevance,* that is, to modernize development approaches to deliver secure, resilient software capabilities within hours or days rather than months or years. Achieving this vision requires a fully automated software production tool chain, linking model-based software engineering to automatic code generation including fully automated continuous integration and continuous deployment, testing (to include developmental and operational), curation of models and simulation environments, and digital twins for experimentation. Such automation will assist in delivering secure, resilient, and defect-free software capability from inception to deployment with frequent software capability releases and a continuous feedback loop, on the order of hours or days in length.

Increased reuse of secure enterprise services and use of open systems architecture will provide efficiencies to increase quality and reduce time for development of new software capabilities into weapons systems. Industrial base partners and programs will share reusable software components while protecting intellectual property and rewarding innovation. As S&T software is developed, new software capabilities will transfer into acquisition systems and programs of record iteratively at increasing velocity.

Figure 1 captures the vision and four strategic goals to support the vision. At the heart of this concept is the need to deliver software capabilities at the pace of demand in support of warfighter needs. Goals are tightly tied to the National Defense Strategy and recommendations from the Defense Innovation Board and Defense Science Board to ensure the Department can transfer effective and relevant software capabilities rapidly to acquisition programs of record, when needed, to support warfighter needs in an ever-changing environment. The strategic goals align with the relevant six sections in the congressional language referenced in Appendix A.

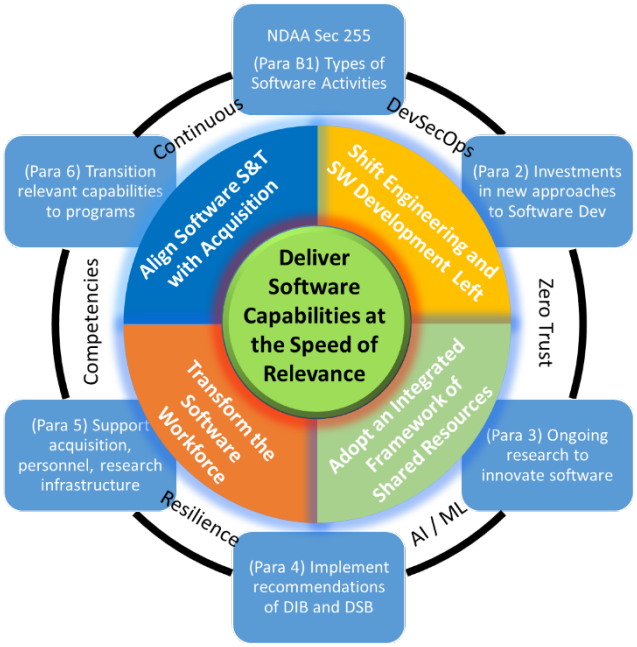

Figure 1. DoD Software Strategic Vision and Goals

Strategic Goals

1. Shift engineering and software development left.
2. Adopt an integrated framework of shared resources.
3. Transform the software workforce.
4. Align software science and technology with acquisition.

Using this strategy, the DSSC intends to work with stakeholders to bridge the gap between software S&T and R&D by adopting a common set of integrated tools, data, and shared resources in support of a more streamlined, rapid, and continuous delivery of new software capabilities into the hands of the warfighter.

The following paragraphs discuss the four strategic goals and their supporting focus areas. Section 3 discusses additional ongoing DoD activities that support the strategic goals and align with the activities listed in NDAA 255 3(b). The DSSC will continue to coordinate with stakeholder COIs to refine the financial and human resources needed to accomplish each goal.

2.1 Strategic 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. Goal 1 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. Figure 2 shows an example of the research, engineering, development, and operations communities working to develop, mature, test, and deliver new capabilities to the end user and warfighter.

Figure 2. Strategic Goal 1: Shift Engineering and Software Development Left

Focus Areas to Enable Goal 1

The following six focus areas enable strategic Goal 1, to shift engineering and software development left.

2.1.1 Advance DevSecOps [8] [9]

DevSecOps is an extension of DevOps software development and operations approach that places extreme emphasis on including cybersecurity resilience within the entire life cycle process. Rather than waiting until a system is entering initial operational capability (IOC) to run security scans, DevSecOps uses a "shift left" approach that incorporates a variety of security equities (e.g., static code analysis scans, dynamic code analysis) within the DevSecOps automated continuous integration (CI) and continuous delivery (CD) pipelines.[10]

The DSSC will facilitate the adoption and expansion of DevSecOps automated CI/CD pipelines as the preferred approach for developing software, delivering secure resilient code, and better connecting software engineering with the Department's S&T research initiatives. Software that follows the DevSecOps reference design[11] will support a smoother transition from S&T to other RDT&E phases (6.4-6.8), providing a more rapid advancement of resilient working software capabilities to the warfighter.

One challenge involves how to continue advancing DevSecOps to support real-time weapon systems where deterministic behavior, safety-critical certifications, and flight certifications may be required. Other challenges for advancing DevSecOps include how to use artificial intelligence (AI) and other emerging technologies to further accelerate the way software is created, improve cybersecurity resilience and software quality, and provide expert systems to more efficiently assist in control gate[12] adjudication within the DevSecOps process itself. To meet these needs, the DSSC will coordinate S&T research activities to advance DevSecOps, connect with software engineering initiatives, and improve support of real-time, cyber-physical weapon system challenges and emerging technology opportunities.

---

[8] *DoD Enterprise DevSecOps Reference Design,* Version 1.0. Nicolas Chaillan, et al., DoD Chief Information Officer, August 12, 2019.

[9] DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops).

[10] "What Is a CI/CD pipeline?" Red Hat, Accessed July 2021. https://www.redhat.com/en/topics/devops/what-cicd-pipeline

[11] *DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes,* Version 2.0. Nicolas Chaillan, Chief Software Officer, United States Air Force, SAF/AQ, March 2021. https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOpsReferenceDesign.pdf

[12] "How Control Gates Can Help Secure the Software Development Life Cycle." (ISC)2 Government Advisory Council Executive Writers Bureau, December 15, 2009. https://gcn.com/articles/2009/12/15/ics2-secure-software-life-cycle.aspx

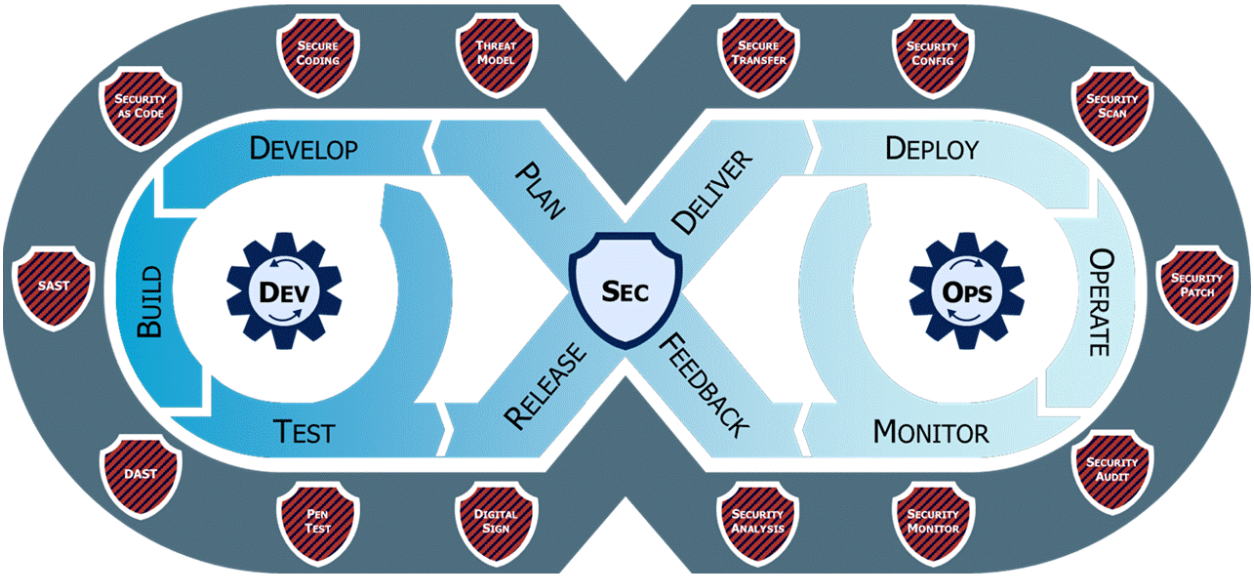

Figure 3. Advance DevSecOps to Deliver Secure Resilient Software

2.1.2 Enhance Resilience Through Speed

Speed functions as risk mitigation supporting Goal 1 in that swifter software updates provide security earlier in the development cycle, allowing less time for vulnerability and thus greater resilience. The DSSC will focus on S&T developments that enhance speed of defect detection and bug fixes using automated CI/CD pipelines, immutable infrastructure, and highly secure hardened containers, assured through resilient cybersecurity and a zero trust architecture (ZTA).[13] [14]

> *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 800-207)

A ZT approach within the DevSecOps reference architecture draws on capabilities that collectively reduce the attack surface and enable rapid detection of vulnerabilities and intrusions.

[13] *Zero Trust Architecture.* Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), and Sean Connelly (DHS). SP 800-207. National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, Maryland, August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[14] "NIST publishes Special Publication (SP) 800-207, 'Zero Trust Architecture.'" *NIST Updates.* National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, Maryland, August 11, 2020. https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

Some of the capabilities include:

- Infrastructure as Code (IaC) – Process of managing and provisioning computer infrastructure through code versus manually intensive, error-prone processes. This process allows rapid creation, configuration, and management of system infrastructure.
- Service Mesh – Middleware providing integration of web services, encryption for all data in flight, access control integration, white listing, and a proxy to log all activity in support of continuous monitoring. A service mesh is vital to ensuring security and maximizing performance within a DevSecOps system.
- Continuous Monitoring – System that aggregates data from a variety of sources including the service mesh and secure containers (via sidecar) to create a complete sight picture of all activity occurring within the system. An advanced monitoring system then examines data packets for vulnerabilities or detection of intrusions, sending alerts to engineers if discovered.
- Secure Containers – A container (e.g., Docker) created with an approved operating environment, attached and securely communicating with a sidecar (e.g., Twistlock), and integrated into the Continuous Monitoring system.

This approach will reduce time to detect and mitigate vulnerabilities to seconds or minutes rather than the typical cycle of days and months within a perimeter strategy.[15] The DSSC advocates resilience through speed using pervasive automation, ZT, and DevSecOps.

2.1.3 Create and Curate High-Fidelity Hardware-in-the-Loop and Software-in-the-Loop Models and Simulations[16] [17]

Software in the loop (SWIL) is a way of using models and simulations (M&S) to test and validate integrated software components. Hardware in the loop (HWIL) is a technique used in the development of complex real-time and embedded systems (e.g., missiles, helicopters, unmanned aerial vehicles). HWIL links the embedded systems to the sensors and actuators using electrical emulation. SWIL and HWIL allow software developers to rapidly test and validate capabilities on simulated virtual and physical models to identify defects more quickly and avoid costly and time-consuming testing on the actual physical platform itself.

High-fidelity HWIL/SWIL environments and M&S allow the Department to shift left by adopting software S&T initiatives sooner in the development process. Programs will integrate HWIL/SWIL simulation capabilities within a software development integrated framework of shared resources to enhance rigor and provide improved confidence of integrated test results. The DSSC will work with stakeholders to champion the use of model-based software and systems engineering, with the confidence and trust needed (built, in part, through feedback loops, blame-free retrospectives, and root cause analysis), for the model to be the authoritative source

---

[15] "Data Breach Response Times: Trends and Tips." Rob Sobers, *Inside Out Security Blog,* Varonis, June 17, 2020. https://www.varonis.com/blog/data-breach-response-times/

[16] "What Is Hardware-in-the-Loop?" National Instruments Corporation, December 17, 2020. https://www.ni.com/en-us/innovations/white-papers/17/what-is-hardware-in-the-loop-.html

[17] "Software-in-the-Loop Simulation." MathWorks, 2021. https://www.mathworks.com/help/ecoder/software-in-the-loop-sil-simulation.html

of truth across the life cycle of activities from concept ideation to disposal. The DSSC supports creating a federated model registry to promote reuse and to maximize visibility of available models across their domain areas, with the models made available to research scientists.

2.1.4 Enhance Engineering Rigor[18]

To enhance engineering rigor, the Department promotes principles including solution fidelity, use of formal methods, separation of concerns, modularity, incrementalism, abstraction, generality, and anticipation of change. DoD will continue to implement digital engineering (DE) and model-based systems engineering (MBSE) practices to improve the quality and depth of engineering representation of solutions under development. The best practices will support accuracy and efficiency and thus support Goal 1 to shift engineering and software development left.

The software factory environment requires pervasive automation to maximize software development velocity while minimizing tedious manual steps. The strategy will include support for automation of alerting CI/CD pipelines, and integration layers between software factory components.

Self-service provides development teams with the means to self-administer software development environments without the need to request actions or submit tickets to a third-party entity (e.g., information technology (IT) administrators). A self-service approach allows DevSecOps teams to quickly react to emerging needs, such as creating new integrations, evaluating new software development tools/capabilities, or addressing broken resources. Self-service typically is achieved through a multifaceted security-focused strategy aimed at maximizing software development velocity while minimizing risk (e.g., ZT, network isolation, artifact monitoring). A self-service approach supports Goal 1 by allowing the development teams to rapidly address emerging issues that otherwise could constrain or delay the software development process.

The DSSC supports the development of digital engineering, model-based software, and systems engineering using automated tool sets to test, validate, and simulate alternative designs and design changes. S&T software development activities will support Goal 1 by employing automation across all aspects of the software factory[19] and project management components to eliminate tedious, manual steps to the maximum degree practicable, enabling higher velocity, consistency, and better quality software components.

[18] "Self-Service Approach to Agile Software Development." Olga Annenko, DZone Agile Zone, September 30, 2016. https://dzone.com/articles/self-service-approach-to-agile-software-developmen

[19] https://dodcio.defense.gov/library/ A DoD DevSecOps software factory includes the people, processes, and tools to enable continuous integration continuous software delivery pipelines in a multi-tenet environment.

2.1.5 Ensure a High Level of Software Assurance

The DSSC will emphasize the importance of achieving a high level of software assurance throughout the software development pipelines and supporting platforms flowing out to the resulting operational software-intensive systems.

Software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. [20]

Software assurance implies secure coding practices, tools, and processes within the software development ecosystem to protect vital assets and adds confidence that the software produced will require minimum rework or rewriting when moving into later phases of RDT&E. The main objective of software assurance is to ensure that the processes, procedures, and products used to produce and sustain the software conform to all requirements and standards specified to govern those processes, procedures, and products. A secondary objective of software assurance is to ensure that the software-intensive systems we produce are more secure.[21]

Rigorous software assurance paired with DevSecOps will produce fewer vulnerabilities and risks and result in fewer fixes and delays across the system life cycle. High-fidelity modeling coupled with automated testing creates confidence that safety-critical systems will maintain high levels of software assurance. Supporting guidance and capabilities include continuous ATO (cATO) process, security technical implementation guide (STIG), ATO inheritance from underlying platforms (e.g., Platform One), and Iron Bank trusted, secure enterprise code and container repository.

2.1.6 Mitigate Technical Debt

The DSSC will support S&T research into areas that contribute to technical debt accumulation and methods of reducing their impact. In software development, technical debt refers to the implied cost of additional rework and risk caused by:

- Poor software architectural decisions that employ poor design considerations (e.g., tight coupling of interfaces or technologies, lack of defensive coding standards).
- Failing to manage the software defect backlog as it continues to grow.

Frequent and iterative mitigation of technical debt is important because unchecked accumulation of technical debt can lead to system stability and performance issues, as well as adding cybersecurity risk. When issues with mismanaged technical debt do begin to surface (e.g., system crashes or slow performance), their correction often leads to unplanned work, taking attention away from planned work, negatively affecting the program's cost and schedule,

---

[20] Foundations for Software Assurance. Carol Woody Dan Shoemaker Nancy Mead, Carnegie Mellon University, May 14, 2013 (revised). https://us-cert.cisa.gov/bsi/articles/knowledge/principles/foundations-software-assurance

[21] "Software Assurance." DAU Acq Notes: Program Management Tool for Aerospace, Software Management. July 31, 2021. https://acqnotes.com/acqnote/careerfields/software-assurance

delaying planned deliverables. For those projects approaching transition to RDT&E, significant levels of unmitigated technical debt can cause a technology to fall into the valley of death[22] because of the time and expense it would take to address. Mitigating technical debt supports Goal 1 by avoiding these potential delays and impediments to progress.

2.2 Strategic Goal 2: Adopt an Integrated Framework of Shared Resources

Goal 2 advocates the use of an integrated framework of shared resources using cloud-native microservices instead of program-specific, monolithic architectures. The DSSC will advocate for research into shared resources to increase collaboration and reuse to prevent redundant, stovepipe development.

Monoliths usually have a single, large tightly coupled code base, making it hard for software developers to understand, and they create a barrier for S&T research scientists to insert new capabilities quickly. Microservices typically provide a well-organized, decoupled, easy-to-understand code base, allowing for more frequent independent deployments of software. This is especially useful for research scientists in the S&T community who are developing new advanced software capabilities, models, simulations, or prototypes, such as a decoupled application to an existing program already in development or sustainment.

Microservices are one part of the overall journey to an integrated framework of shared resources. Figure 4 illustrates the framework of three layers of shared resources starting with the largest primary layer of highly resilient, cloud-native DevSecOps infrastructure environments. Microservices exist within the second layer, within the Federated Repsitories of Programs, Models, Data and Software. This layer will offer a template-driven highly curated environment with a variety of integrated tools, services, and capabilities. The top layer represents the holistic "value-added" S&T software development environments across the Department.

[22] The expression "valley of death" refers to the fate of promising science and technology research that languishes in laboratories rather than making the transition to programs of record or capability delivered to the warfighter.

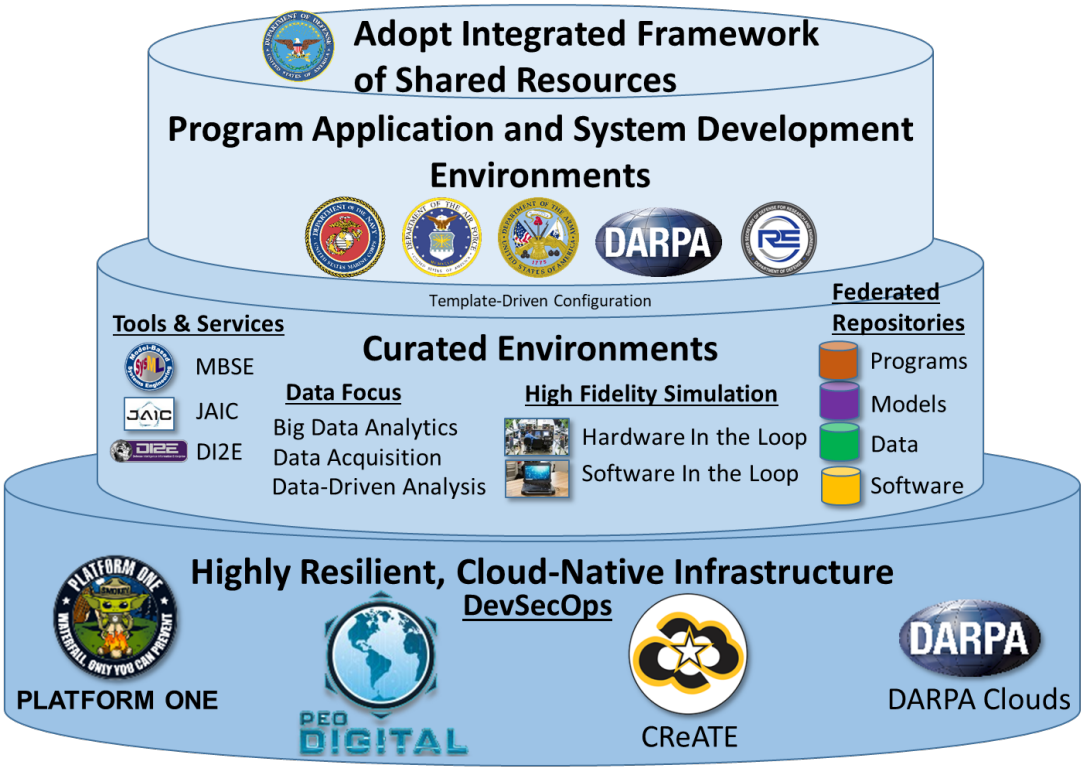

Figure 4. Strategic Goal 2: Adopt an Integrated Framework of Shared Resources

Focus Areas to Enable Goal 2

The following six focus areas enable strategic goal 2, an integrated framework of shared resources.

2.2.1 Research Highly Secure, Resilient, Cloud-Native Architectures

Cloud-native architectures offer significant advantages (e.g., reliability, elasticity, security) and provide a robust infrastructure in support of DevSecOps but are typically used only on business and command and control systems. Moving from a monolithic architecture and design approach with security bolted on at the end, to a virtualized hypervisor-driven[23] computing infrastructure or platform as a service (PaaS), with built-in security, supports the ability to deliver rapid highly resilient software capabilities to the warfighter at the speed of need, to support mission execution.

The DSSC recognizes recent gains with prototype projects conducted by the Navy and Air Force related to using a Cloud-native/edge computing approach within real-time systems, and recommends additional research be conducted to maximize adoption across all Services and warfighting domains.

[23] A *hypervisor* is computer software that runs virtual machines (VMs).

Using cloud-native microservices to iteratively create highly robust and secure services, infrastructure, and applications will minimize complexity, provide faster distribution time, reduce attack surfaces, enable functionality shielding, and lessen complexity, producing more cohesive code structures. S&T initiatives must research legacy system modernization approaches (e.g., Strangler Pattern, adapters) to extend a system's capabilities, boost architectural resilience, and enable accelerated delivery of software capabilities to the warfighter while maximizing cost/schedule benefits.

Cloud-native microservice designs provide loosely coupled applications that are fine-grained with highly secure, lightweight, and robust protocols. Microservices and domain-driven designs[24] enable the CI/CD of code at the speed of relevance. The concept of domain-driven design eases the creation of complex software applications by connecting the related pieces of software into an ever-evolving model. Creating and modifying domain models emphasizes continuous integration and eases communication across the stakeholders. These models improve flexibility, allowing for modularity and encapsulation. Domain models deliver applications accurately suited for representatives of a domain itself, versus pure user-centered interface design.

2.2.2 Leverage Modern Ecosystems, Technologies, Tools, and Processes

The primary focus of the ecosystem is to rapidly provide an integrated software development, modeling, test, data, and simulation environment (or the ecosystem appropriate for each S&T program) that can be deployed to or accessed by a developer desktop or laptop (physical or virtual). The deployment should be capable of being installed, functional, and interoperable with all software management, configuration management, software build, and deployment pipelines, configurations, and processes, within minutes to hours.[25]

Enabling modern ecosystems earlier within a program life cycle is vital to the DSSC strategic vision and will ensure S&T programs have resources and processes needed to develop software in a manner and on pace with commercial industry and Silicon Valley startups. Use of modern processes (e.g., Lean Agile, AI/ML) will allow programs to rapidly and iteratively develop highly resilient software capabilities that can be transitioned to acquisition with higher velocity, avoiding costly rewrites and reverse engineering, sometimes needed to adapt an S&T developed initiative into a production-ready environment.

---

[24] Domain-Driven Design is an approach to software development that centers the development on programming a domain model that has a rich understanding of the processes and rules of a domain. The name comes from a 2003 book by Eric Evans that describes the approach through a catalog of patterns. Since then a community of practitioners have further developed the ideas, spawning various other books and training courses. The approach is particularly suited to complex domains, where a lot of often-messy logic needs to be organized. By Martin Fowler, April 2020.

[25] See *The Unicorn Project: A Novel about Developers, Digital Disruption, and Thriving in the Age of Data,* Gene Kim, IT Revolution Press, November 26, 2019. Development environments took months to onboard new software developers due to the various silos of each software development capability owner (e.g., configuration management, database A, application B). Each software developer had a slightly different environment from the others, potentially leading to software-related defects and the "it worked fine on my computer" syndrome.

The ecosystem must support a wide variety of software-specific domain areas (e.g., cyber-physical, real-time, C4ISR), modern software approaches (imperative, declarative), languages (e.g., Go, Rust, Scala, C++, Java, Python), and system architectures (e.g., x86, Advanced RISC Machines (ARM), Field Programmable Gate Array (FPGA), Graphic Processor Unit (GPU), Neural Processing Unit (NPU), Tensor Processing Unit (TPU), PowerISA). The DSSC will ensure the ecosystem supports evolutionary architecture and design principles with a strategy to allow technologies to be added, enhanced, or replaced rapidly as needed.

2.2.3 Focus on Data Acquisition, Data Science, and Event Streaming

Data acquisition, integrity, warehousing, analysis, cleansing, curating, and science are critical to supporting the Department's needs. The DSSC will coordinate with the Chief Data Officer (CDO) to ensure scope and breadth of Department activities are adequately addressing development of data access control, assurance, security, and curated databases to enable Department-wide AI/ML and other data science initiatives. Future S&T software initiatives will require use of big data analytics, of structured, semi-structured, and unstructured data sets, to extract information not easily obtained by traditional data processing techniques. The DSSC will coordinate the utilization of modern data-centric S&T initiatives, and advocate implementation of event streaming, where appropriate, through exposable application programming interfaces (APIs) to easily share real-time data (e.g., push notifications, policy or registry updates). The DSSC will support efforts to ensure digital data storage is abundant and easily but securely accessible. Programs and S&T activities will use an integrated framework of shared resources so data can be shared, accessible, and used by research, development, and operational communities seamlessly. The DSSC will seek to eliminate or minimize costly manual effort and human intervention in all aspects of data collection, analysis, reporting, and retrieval activities.

2.2.4 Accelerate Delivery and Adoption of AI/ML

At its simplest form, artificial intelligence[26] (AI) is a field that combines computer science and robust data sets to enable problem solving. It also encompasses subfields of machine learning (ML) and deep learning, frequently mentioned in conjunction with AI. Certain AI algorithms can function as expert systems that make predictions or classifications based on input data.

According to Andrew Ng, Stanford professor and co-founder of the MOOC (massive open online course) provider Coursera, AI is the new electricity. Its impact on society will transform the world in a way similar to the transformation brought about by electricity in the last century.[27] Use of AI in industry is becoming prominent across the commercial sector today (e.g., Tesla self-

[26] "(What Is) Artificial Intelligence." IBM Cloud Education, IBM, June 3, 2020. https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

[27] "Why AI Is the New Electricity." Andrew Ng, Graduate School of Stanford Business, March 11, 2017. URL: https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity

driving cars,[28] Tesla Bot,[29] Apple Siri, Amazon Alexa, Boston Dynamics Atlas[30]) and is being incorporated into the Department's warfighting capabilities.[31] One way the Department has recognized the trend is through establishment of the Joint Artificial Intelligence Center (JAIC), DoD's AI Center of Excellence that provides critical expertise to help the Department harness the power of AI. [32] The JAIC integrates technology development with the requisite policies, knowledge, processes, and relationships to ensure long-term success and scalability.

The spread of AI[33] and automation technologies disrupted more industries than global economists and military leaders expected. These technologies are finding their way into weapon system programs at unprecedented rates. All Military Departments are employing some level of AI in their ecosystems by first understanding and structuring the input data that train AI algorithms. Understanding and structuring the data are key to implementing AI/ML.

2.2.5 Create Federated Portal for Reusable and Shared Resources

For S&T, there are currently limited means and no single point of reference to visualize and understand detailed program information on planned or in-progress capabilities under development in support of shared resources and reuse.

As noted, DoD has adopted DevSecOps and moved from a monolithic to a microservices approach, in which software is delivered in units known as enterprise services with a strong focus on the value of reuse. The current lack of visibility across planned and in-progress programs, paired with a cumbersome, non-responsive search capability, significantly constrains this enterprise goal.

The DSSC envisions a DoD-wide, federated portal that provides a singular point of reference using a modern, highly responsive user interface (UI)/user experience (UX) to allow DoD acquisition programs to have greater details and insight into S&T portfolios and bolster sharing of reusable resources (e.g., data, models, software, enterprise services).

The DSSC seeks to create and maintain a common, federated portal that will house a registry of reusable and shared S&T resources to support visibility of current and developed capabilities to other S&T, acquisition, and operations activities, across the Department.

The portal will use a resilient, yet modern, responsive website framework (e.g., Express, Django, React, Angular), which implements leading web-based UI/UX design patterns (e.g., pagination,

[28] "Artificial Intelligence & Autopilot." Tesla. https://www.tesla.com/AI
[29] "Elon Musk Says Tesla Bot Prototype Will Be Ready Next Year. Can We Believe Him?" Eric Mack, c|net, August 26, 2021. https://www.cnet.com/news/elon-musk-says-tesla-bot-prototype-will-be-ready-next-year-can-we-believe-him/
[30] "Inside Boston Dynamics' Project to Create Humanoid Robots." Ben Dickson, *Venture Beat,* August 27, 2021. https://venturebeat.com/2021/08/27/inside-boston-dynamics-project-to-create-humanoid-robots/
[31] "In a First, Air Force Uses AI on Military Jet." Aaron Gregg, *The Washington Post,* August 16, 2020. URL: https://www.washingtonpost.com/business/2020/12/16/air-force-artificial-intelligence/
[32] "Joint Artificial Intelligence Center - Vision: Transform the DoD Through Artificial Intelligence." DoD CIO. https://dodcio.defense.gov/About-DoD-CIO/Organization/jaic/
[33] "Artificial Intelligence (AI) – Machine Learning (ML) Roadmap." Jill Crisman, Ph.D., Office of the Under Secretary of Defense for Research and Engineering, May 22, 2020.

autocomplete, tagging, progressive disclosure) to provide authorized users (clients) with integrated, interactive capabilities to support rapid search and drill-down on S&T activities, attributes, and reusable applications and services, to include a lessons learned and best practices repository or searchable wiki. The administration UI/UX used by S&T program owners must allow users to easily create or update program information, or add and update shared resources as needed.

The DoD-wide federated portal ecosystem must be highly extensible to rapidly add new applications and capabilities as new technologies evolve and program needs change.

2.2.6 Invest in Low-Code, No-Code, and Robotic Process Automation

Robotic process automation (RPA) is a revolutionary emerging technology that enables automation of tedious, highly manual, repetitive processes to streamline enterprise operations, allowing users to focus on higher priority tasks. RPA is intended to allow work that would take weeks or months to be accomplished in minutes to hours. RPA is scalable to meet fluctuating trends in workload.

The DSSC will encourage the Department to invest in technologies to "democratize"[34] software development, data analysis/curation, and ML experimentation given the growing gap between the demand and availability of highly trained and educated digital talent including software developers, data scientists, and ML engineers. The DSSC promotes creating tools that make low/no-code and RPA solutions safe, secure, and resilient to build and deploy to operations.

Commercial industries are realizing benefits by employing low/no-code and robotic process automation tools. This allows the digital natives that are already in the workforce to implement significant digital capabilities without the need for highly trained software engineers and developers. RPA can eliminate the tedious, menial labor, and allow the existing workforce to focus on the more strategic and differentiated tasks within their day-to-day activities, improving overall productivity, providing more value to the Department.

2.3 Strategic 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. DoD must accelerate the use of new technologies to enhance the identification, recruitment, retention, and development of a superior S&T and software engineering workforce.

The Department must compete to hire, train, and retain software engineers, platform engineers, data 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

[34] Democratized software allows more personnel, especially those at the edge, to use resilient cloud-based data storage, tools and applications to solve front line problems.

software personnel to manage the DevSecOps tech stack and "undifferentiated heavy lifting"[35] so research scientists can focus on innovation, advancing the technology, algorithm, and code development. Figure 5 is an example of typical interactions among DoD personnel, academia, and industry to deliver advanced software-enabled systems to the warfighter.

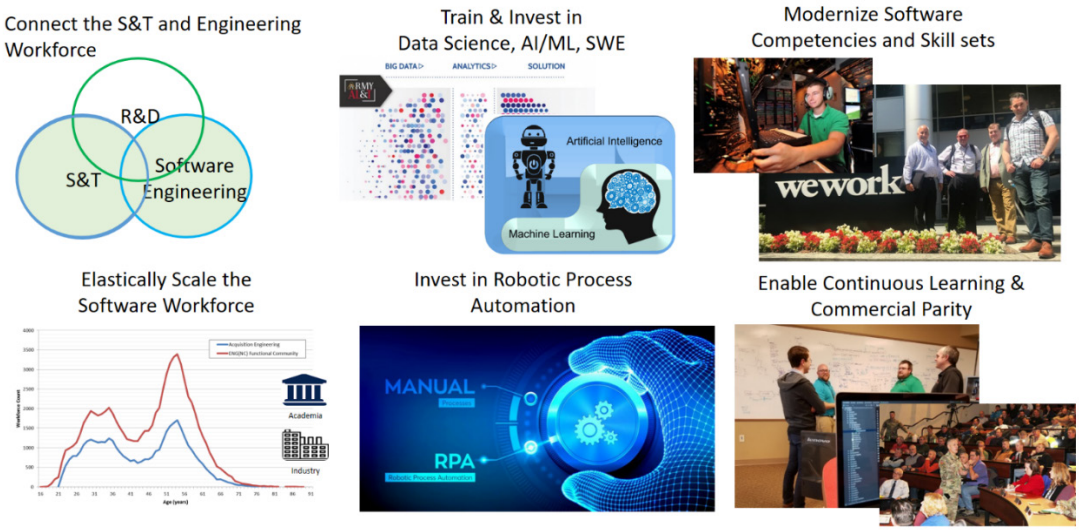

Figure 5. Strategic Goal 3: Transform the Software Workforce

Focus Areas to Enable Goal 3

The following five focus areas enable strategic goal 3, to transform the software workforce.

2.3.1 Connect the S&T and Engineering Workforce

The DSSC will promote organizing the DoD workforce so software engineers, data scientists, and research scientists work alongside one another, on collaborative, tightly coupled teams. The DSSC will promote integrating S&T as opposed to considering it an independent function or workforce.

Innovation and advanced capabilities will transition more quickly to programs of record when research scientists and software engineers are collaborating and using an integrated framework of shared resources in a cloud native ecosystem. This integration will provide a smooth transition within the pipeline to move R&D results toward production use. Use of modern technical stacks, modern architectural approaches (e.g., microservices), and other enabling considerations (e.g., data availability, resource sharing, software reuse, abstraction layers, high-fidelity modeling and simulations) will increase systems engineering rigor, alignment, and velocity across the

[35] Coined by Amazon Web Services Chief Technology Officer, associated with configuring and managing the required information technology (IT) infrastructure, often attributed to 70 percent of the non-mission-related non-value-added IT work, so research scientist and developer can focus on code development and delivering new capabilities that add value to the mission.

Department. Security orchestration and test automation will be persistent, so research scientists can focus on advancing the technology and inserting new software capabilities continuously.

2.3.2 Train and Invest in Data Science, AI/ML, and Software Engineering

The DSSC will focus on adopting AI and data science within the software engineering function. It will promote DoD investment in data acquisition, warehousing, cleansing, and curation of big data to enable ML and the development of new AI algorithms.

AI will be the next "Manhattan Project."[36] Not only will DoD require significant investment in AI training, infrastructure services, and resources, but the entire DoD culture will need to change to become "data acquisition centric" and "data quality driven." The training, infrastructure, and resources will be useful only if DoD possesses abundant high-quality data and personnel with the skills to exploit that data.

2.3.3 Cultivate a Leading S&T and Software Engineering Workforce

The DSSC will work to ensure a sufficient subset of the S&T and software engineering workforce is skilled in modern software development practices, or has access to such expertise. Workforce initiatives will ensure high cohesion among software research, development, security, testing, and operations personnel. The DSSC will continue to develop recommendations for modernized software competencies informing Defense Acquisition University (DAU) training, certification, and credentialing.

The USD(A&S) "Back to Basics" memo[37] directed the consolidation of multiple acquisition workforce career fields into six functional areas to streamline the defense acquisition workforce certification and governance construct. To advance modern software development practices within the new construct, software acquisition competencies must be amplified in each of the six new functional areas. In addition, the silos created by the original career fields are counter to the DevSecOps culture. All engineers must understand cross-functional roles and apply their skills across the entire mission life cycle. The culture must change and silos need to be broken down.

Modern software development competencies and skill sets for DevSecOps software engineers, coders, cybersecurity specialists, testers, and research scientists need to be advanced by the Service components beyond the very high level Tier 1-3 functional area competencies. The functional area competencies are so high level they provide only an introductory understanding of DevSecOps. Deeper learning, knowledge, skills, and abilities are needed. OUSD(R&E) tasked the RAND Corporation (an FFRDC) to investigate three areas to help improve the Department's ability to rapidly and reliably deliver complex software-dependent capabilities. The first area was the development of a competency model that emphasized an enhanced understanding of modern software practices and technical competencies. The second was to review training and education offerings at the DAU and identify potential gaps in the current

[36] *Future of Defense Task Force Report 2020,* House Armed Services Committee, September 23, 2020.
[37] "Back to Basics for the Defense Acquisition Workforce," Under Secretary of Defense for Acquisition and Sustainment Memorandum, September 2, 2020.

training. The third was to recommend options for tracking and managing a software acquisition workforce. RAND developed a model consisting of 48 competencies[38] that serves as a foundation for future software workforce functional area competency updates and training. Continuous learning, pairing with experts, relevant commercial courseware, on-the-job-training, and experience will hone specialized skill sets and talent.

2.3.4 Enable Continuous Learning to Keep Pace with the Commercial Sector

A Government employee's professional development relies on continuous learning, through activities such as brown bag sessions, technical interchange meetings, commercially available online learning platforms (e.g., Air Force's Digital University, Coursera, Udacity, Udemy), communities of practice, and workforce pairing to share best practices and knowledge across or between teams, to enhance and develop software skill sets across the workforce. DAU training provides significant value across DoD-unique competencies and processes. Due to the wide availability of low-cost, world-class commercial offerings (e.g., Coursera, Udemy) across emerging modern software development and digital engineering domains, DAU has committed to partnering with select commercial vendors to provide DoD with some of the highest quality technical training from leading subject matter experts in their respective fields.

The DSSC will promote building professional experience through pairing and on-the-job-training with commercial sector experts. This will promote and enhance competence in building DevSecOps teams that are self-motivated and leverage individual continuous learning, as technology stacks from 2 years ago (for example) may already be obsolete. Demand for DevSecOps engineers and Data Science professionals continues to surge, creating a scarcity of talented individuals. The modern software development landscapes continue to change at a very rapid pace, and therefore, the DSSC will support reevaluation of course offerings at regular intervals.

2.3.5 Elastically Scale the Software Development Workforce

The key elements of an elastic software workforce are drawn from industry experience and include structural and behavioral agility combined with foundational and functional technology support. Workforce agility can be achieved by improving the integration of workforce sources with work centers that provide the right set of skills and staff at appropriate times. DoD already draws on multiple staffing sources including those from the Government, research labs, and industry contractors to meet software S&T needs. Realizing the benefits of an elastic software workforce will rely on innovation and flexibility in leveraging those sources and keeping them at the technological edge. The DSSC will collaborate across the Department to strengthen and enhance the central pillars of this approach: talent cultivation, partnerships, and improved Government hiring.

[38] "Software Acquisition Workforce Initiative for the Department of Defense: Initial Competency Development and Preparation for Validation." Sean Robson, et al., Washington, D.C.: RAND Corporation, 2020. https://www.rand.org/pubs/research reports/RR3145 .html

DoD will never be able to "out-spend or out-hire"[39] its adversaries, or even the commercial sector. A process to cultivate leading talent and elastically scale is necessary. DoD can offer other incentives including valuable experience, rewarding challenges, and positions of responsibility. The scarcity of cleared software talent[40] needs to be addressed as the security clearance process alone can take up to 18 months. Estimates provided by the Bureau of Labor Statistics[41] indicated there were more than 1.5 million software developer jobs in the United States in 2020. While there is no accurate measure of a software development workforce in DoD, estimates fall between 30,000 and 50,000 Government employees,[42] a fraction of the 1.5 million nationwide. Clearly, DoD is not driving the demand and size of the software development workforce nationwide. Nevertheless, DoD is competing for the same talent the commercial sector is attracting. The DSSC will promote the Department's effort to upskill the software development workforce and improve the hiring process to onboard technical talent. DoD needs to invest in creating a software workforce that can lead by enforcing strong architectural and security assurance criteria.

One important source of talent development is through early stage interaction and partnerships with universities, to develop training and opportunities for university researchers. The DSSC will work with partners to promote internships and job fairs with universities and engage on social media to reach out to graduates and the younger members of the workforce. Recruiters will communicate the value of Government experience, civil service, and the opportunity to obtain a security clearance. The DSSC promotes the application of financial incentives to hire experienced software talent while offering horizontal and vertical mobility.[43] The DSSC encourages partnerships in which government employees team with contractors in the commercial IT, cyber, and software development workforce, and scale when needed with contractors to perform functions that are not inherently governmental.

The DSSC will actively support the establishment of a software engineering career field (or functional area) for both military and civilian personnel. The DSSC will work through DoD channels to partner with OPM for the establishment of a new occupational series for software engineering outside the existing 2210 (IT Management), 1550 (Computer Scientist), and 0854 (Computer Engineering) occupational series roles. A civilian software career track will focus on all elements of software development, to include: Product Designer (User research, UX, UI, visual design); Product Manager/Owner; Data Scientist; Data Engineer; Software Engineer/Developer; DevSecOps Engineer; Cybersecurity Engineer; Network Architect/Engineer; and/or Platform Engineer. These new series will focus on finding,

[39] "Cybersecurity and Cyber Operations S&T Roadmap." Daniel J. Ragsdale, Ph.D., Office of the Under Secretary of Defense for Research and Engineering, June 22, 2020.
[40] "Software Productivity Trends and Issues." *Defense Acquisition Research Journal* 27(2) Issue 92, April 2020.
[41] *Occupational Outlook Handbook.,* Bureau of Labor Statistics, U.S. Department of Labor (Software Developers), September 1, 2020.
[42] *Software Industrial Base Assessment: Phase I Report.* Center for Strategic and International Studies, Washington, D.C., October 4, 2006. At the time the study estimated 13,000 DoD Government and 68,000 cleared contractor software developers.
[43] Ability to work with other teams on new projects and programs, and promotion / increased pay.

attracting, retaining, and prioritizing the right people for the needs of Commands. A clear career progression and promotion potential roadmap will be included.

Congress granted federal agencies flexibility in hiring and recruiting, where there is a vital need for certain positions. The Office of Personnel and Management (OPM) describes more than 20 positions on its website that have Government-wide Direct Hire Authority (DHA), including critical STEM and cyber positions.[44]

The DoD has several DHAs and Expedited Hire Authorities (EHA) granted by Congress through NDAAs. Within DoD, it takes an average of 200 days to hire a candidate through DHA or EHA, though OPM guidance calls for less than 70 days to make a hire.[45] As the DoD looks to recruit highly sought-after software engineers, DevSecOps engineers, cybersecurity specialists, data scientists, and electronics engineers, it needs to address the protracted 6 to 9-month hiring process as this lag deters potential candidates.

The DSSC will facilitate the practice of embedding HR professionals in software-intensive units or program offices that are cross-trained with a working-level knowledge of technical competencies such as software development and cybersecurity. In addition, technical hiring managers will have a better understanding of basic DoD HR procedures to expedite and complete the hiring process but not do the HR job for them.

By attacking these three areas the DSSC will systematically enable workforce improvements that will enhance technical currency and increase the flexible application of DoD software S&T professionals to mission needs. This approach will build a solid connection from research to operational transition of mission-driven software capabilities.

2.4 Strategic 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. Creating technical advancements in complex weapon systems is never an easy or low-risk venture, but still too many S&T initiatives will not bridge the valley of death.

Figure 6 is just one of many illustrations used to define the critical transition phase to acquisition. The DoD acquisition system must be flexible, confront the transition risk, and bridge the valley from concept exploration to acquisition. Many software S&T projects need to be better aligned and connected with acquisition programs of record.

Software engineering experts in the Department are often given the formidable task of implementing R&D code into weapon systems. The difficulty of the task is not always

[44] "Direct Hire Authority." U.S. Office of Personnel Management. Accessed October 14, 2019. https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority.
[45] "Direct Hire Authority Fact Sheet." U.S. Office of Personnel Management. Accessed October 14, 2019. https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Fact-Sheet.

appreciated. Reusing or refactoring R&D software into a production-ready system can take years and cost millions of dollars. R&D code is typically developed to demonstrate a proof of concept or a prototype capability and is usually delivered immature and with a high level of technical debt. Depending on the amount of technical debt and refactoring needed, an R&D initiative may not transition at all, in part due to the cost. Software is software; there should be no difference between R&D code and production code. Yet, too many R&D programs do not spend their valuable Technology Maturation and Risk Reduction (TMRR) schedule to hone a software factory and processes to produce production grade code.

Acquisition regulations governing competition prior to entering a program Engineering and Manufacturing Development (EMD) phase can hinder forward progress and a smooth transition from TMRR to EMD. Use of the new Software Acquisition Pathway Policy[46] will help mitigate many of these types of acquisition challenges, if in fact hardware and software development can be effectively separated, and high-fidelity modeling and simulations provide an authoritative source of truth. The Software Acquisition Pathway was built to support rapid technology innovation and alignment with commercial approaches. Its central design principle is the use of rapid, incremental cycles, supporting incremental technology investments that break the adversary's Observe, Orient, Decide, Act (OODA) loop by shortening internal cycle times. These short, frequent cycles are designed to be more responsive to changing technologies, operations, and threats. Strategic goals 1, 2, and 3 provide the foundation to enable the transition of new software capabilities to acquisition.

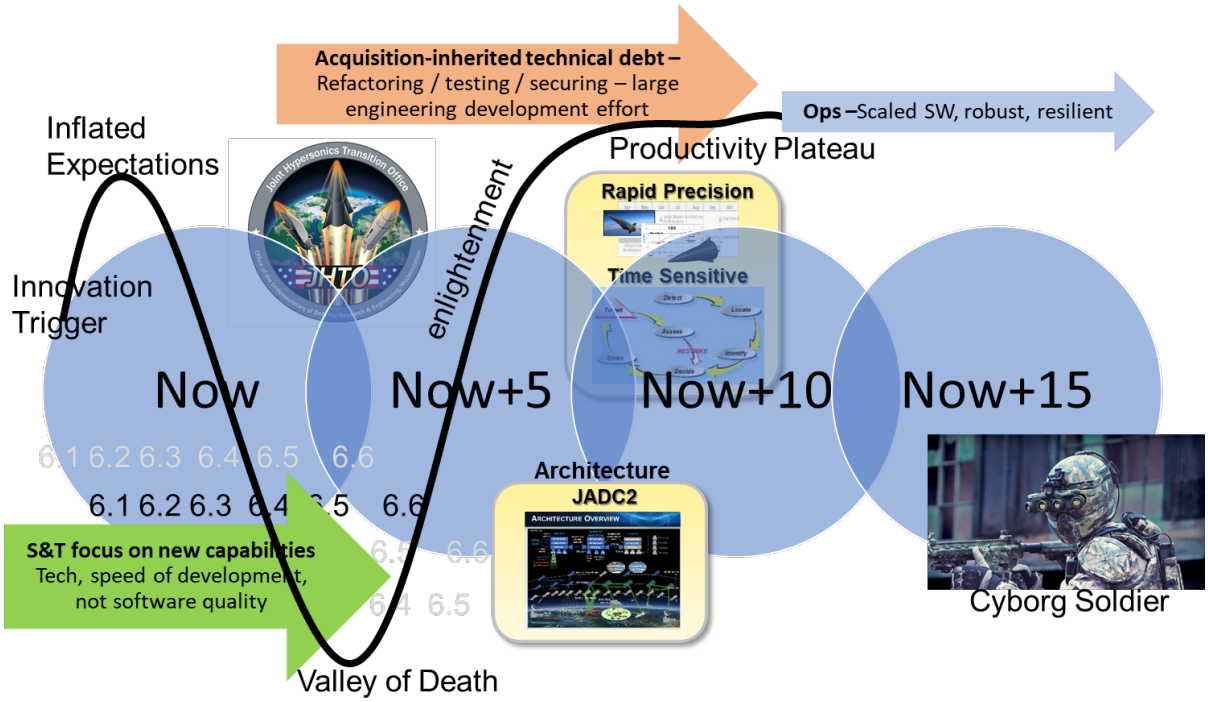

Figure 6. Strategic Goal 4: Align Software S&T with Acquisition

[46] DoD Instruction 5000.87, Operation of the Software Acquisition Pathway. Office of the Under Secretary of Defense for Acquisition and Sustainment, October 3, 2020.

Focus Areas to Enable Strategic Goal 4

The following five focus areas enable strategic goal 4, to align software S&T with acquisition.

2.4.1 Bridge the Gap Between S&T and Acquisition

The Department needs to create a cohesive working relationship between S&T and acquisition programs in support of aligning and modernizing the software development processes used by research scientists. The DSSC will work with the S&T community to focus on innovation, small business innovative research (SBIR), early 6.1, 6.2, 6.3 S&T, and low Technology Readiness Level (TRL) activities to deliver software into a DevSecOps pipeline or a Government laboratory software factory.

2.4.2 Embrace the Mindset that Software Is Never Done[47]

The DSSC will focus on an evolutionary approach to architecture and design. The approach will implement services, capabilities, and integrations via highly efficient abstraction layers (e.g., reverse proxy) to maximize a technology agnostic approach, wherever possible, allowing rapid replacement of technologies and capabilities throughout the S&T life cycle, blending S&T with development.

2.4.3 Advocate a Strategic Outlook toward S&T Investments

The DSSC will work with stakeholders to create a federated sight picture for all software S&T investments. The DSSC promotes a venture capital-like investment strategy. The DSSC will advocate research into additional investments like public/private non-profit partnerships to focus on investigating, curating, and employing the latest cutting-edge technologies and capabilities into S&T programs. The DSSC will work with partners in DoD to ensure laboratories, FFRDCs, universities, and contractors deliver reusable code while protecting Government purpose rights and intellectual property. An essential component of the Department's Strategic Outlook will be the expanded used of Open Source Software (OSS). The DSSC will work to facilitate the expansion of safe OSS use by extending automated cyber resilience tools to ensure the integrity of OSS adopted for use in Government systems. This includes S&T investments needed to build the expertise necessary to transition software into programs and to return improvements back to the open source community.

2.4.4 Invest in Leap-Forward Tech to Leverage Industry Best Practices

The DSSC will work to identify and advocate ongoing investments in cloud-based infrastructure and services to enable new S&T software development including AI/ML and to leverage JAIC initiatives, automation, microservices, DevSecOps pipelines, and modern tool sets. This will facilitate improved DoD adoption and utilization of commercial best practices and their rapid capability release cycles. The DSSC will support ongoing efforts to identify and fund new

[47] "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage." Defense Innovation Board, Washington, D.C., May 3, 2019.

approaches toward securely removing integration barriers that constrain use of commercial open source and COTS[48] technologies within weapon systems. This effort includes ongoing research and identification of commercial innovations applicable to DoD needs.

2.4.5 Streamline the Planning, Funding, Requirements, and Contracting Process

The S&T and R&D process is not always connected with funded programs of record. Contracting for R&D without a software development and reuse strategy can lead to accumulated technical debt and difficulty bridging the valley of death.

The DSSC will work across Department S&T activities to support investments that focus on warfighter collaboration while still allowing unconstrained innovation and development of new and novel technologies. The Government still determines which projects to fund and accomplish in-house versus acquire. If acquiring, it should maximize use of the Software Acquisition Pathway for software development.

[48] Commercial-off-the-shelf (COTS) products include hardware and software solutions, including installation, training and cloud services associated with COTS packages.

3 NDAA 255(b): Software S&T Strategies for R&D of Next Generation Software

Section 2 discussed the Department's strategic vision, goals, and focus areas for developing next-generation software and software-reliant systems across the entire lifecycle. This section presents ongoing and planned strategies to support and accelerate DoD software S&T consistent with the strategic goals and focus areas.

DoD RDT&E funding is provided through Title IV, which includes appropriations for the Army, Navy, Air Force, Space Force, a Defense-wide RDT&E account, and the Director of Operational Test and Evaluation. Space Force is a new account included in the FY 2021 request. The Defense-wide account includes the Missile Defense Agency (MDA), Defense Advanced Research Projects Agency (DARPA), Office of the Secretary of Defense, and 15 other DoD organizations. Within each of these accounts are program elements (PEs) that provide funding for particular activities.

RDT&E funding is typically organized through eight categories with a budget activity (BA) code 6.1 through 6.8. Of these, BA 6.1 Basic Research, 6.2 Applied Research, and 6.3 Advanced Technology Development are referred to collectively as the DoD Science and Technology (S&T) budget. In FY 2020 the S&T budget accounted for $16.12 billion (15.3%) of DoD RDT&E funding[49]. This portion is often seen as the budget pool necessary to develop knowledge of future military systems and drive long-term innovation.

To maintain technical superiority on the battlefield, the Department relies on S&T knowledge developed in large measure through DoD-funded research performed by industry, universities, federal laboratories, and others. DoD S&T must push the limits of technology to generate breakthroughs in basic science, research, development, and engineering. RDT&E under budget activities 6.4-6.8 focuses more on generating and delivering an end product but may have its origins in S&T.

Figure 7 illustrates how the Department-wide Software S&T Strategy can inform research across BA 6.1-6.3 to deliver advanced capabilities and better software to the warfighter more quickly.

The DSSC will coordinate, collaborate, and align activities across the Department consistent with the technologies described in Section 2. The S&T Senior Steering Group (SSG) will evolve into an ongoing S&T SSG that reaches out to relevant groups (Service S&T COIs, laboratories, etc.) to continue developing the strategy and technology areas at the pace of change.

[49] CRS Reports. Congressional Research Service, November 25, 2020. Crsreports.congress.gov

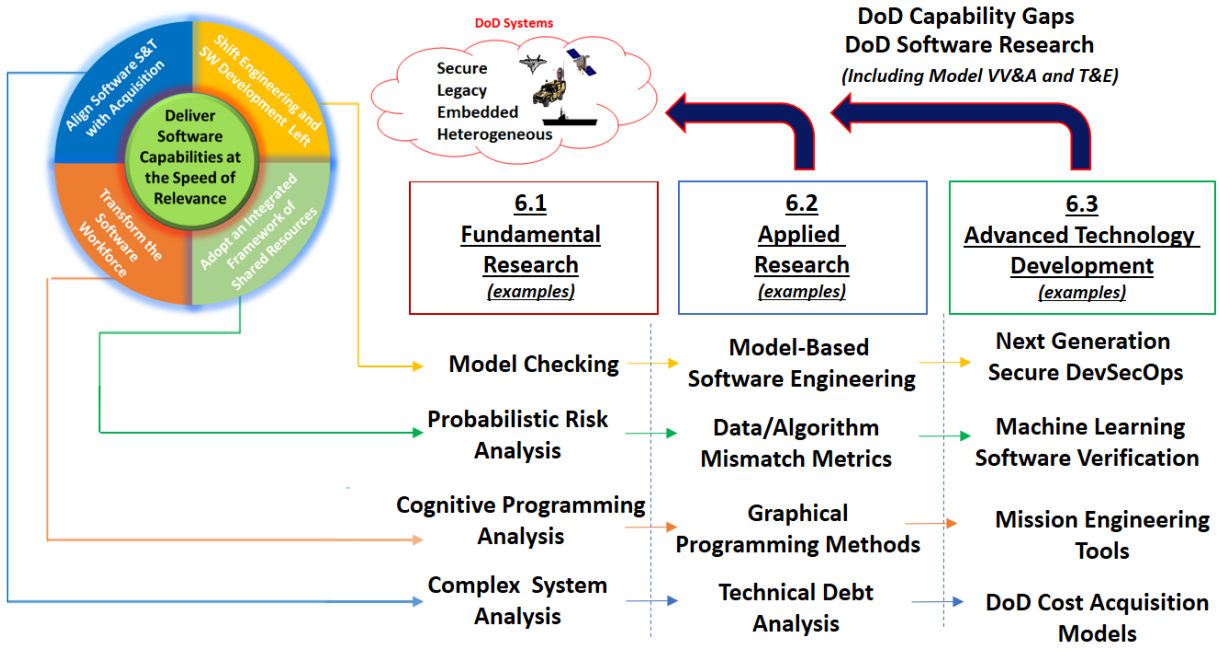

Figure 7. Integrating Software S&T and Acquisition

3.1 Types of Software-Related Activities within the Science and Technology Portfolio of the Department

DoD S&T continually seeks out new and next-generation[50] capabilities to create an overmatching advantage against threats. For software development, the DoD S&T community needs to achieve parity with the commercial sector (cloud adoption, Agile/DevSecOps, automation). Commercial software development companies are currently delivering thousands of releases per day while typical DoD software releases occur in months to years for programs of record in sustainment, and even longer for software S&T activities.

Although S&T activities have made few advances toward commercial parity, the transformation is evident and has started across all of the Services. The Navy developed several modernization initiatives including Compile to Combat in 24 Hours[51], and a Digital Integration Support Cell (DISC) that is developing the Digital Warfighting Platform (DWP)[52]. The Air Force developed a number of modernization initiatives and pathfinders, along with supporting infrastructure

[50] "Given today's globalized access to knowledge and the rapid pace of technology development, innovation, speed, and agility have taken on a greater importance. The Defense Department serves as an innovative leader in developing technology to protect Americans and troops - on and off the battlefield." Department of Defense News, Science and Technology (archive): https://dod.defense.gov/News/Special-Reports/0715_science-tech/

[51] Distribution Statement D. Distribution authorized to the Department of Defense and U.S. DoD contractors: "Digital Transformation and Compile to Combat in 24 Hours" (C2C24). Richard W. Jack. Presentation to the Senior Steering Group, Naval Information Warfare Center, August 19, 2020.

[52] The DWP will revolutionize Naval warfare systems by eliminating stove piped architectures and one-off point-solution integration projects, leverage micro services, Application Programming Interfaces, and Software Development Kits to prioritize integration, interoperability, scalability, and modularity in all software design efforts. https://docs.house.gov/meetings/AS/AS26/20200311/110655/HHRG-116-AS26-Wstate-GeurtsJ-20200311.pdf

components such as Iron Bank, Cloud One, Platform One[53] in support of their DevSecOps reference architecture.

U.S. Navy acquisition professionals recognized the need for a refocused approach to R&D, stressing agility and technical innovation to expedite technological solutions to the warfighter through prototyping and experimentation efforts. The Navy is using the USS Monterey as a digital pilot ship project to transition valuable technology to the fleet. USS Monterey's hardware/software suite will enable unified management of cyber-secure, expandable, compute/network/storage for hardware configuration and application deployment to be scripted, making installation, operation, and maintenance of the shipboard systems less complicated and faster for our Sailors. The project provides a digital twin of the system for initial training of the ship's crew and used OTA contracts as a means to rapidly and iteratively prototype combat system components.

The Army Enterprise Cloud Management Agency (ECMA) is responsible for the Army's cloud modernization strategy. ECMA transitions existing Army software applications into the enterprise cloud solution CReATE while promoting DevSecOps and cloud-native development throughout the Service. ECMA is transforming the Army's approach to software development by enabling program offices and cross-functional teams to pivot to secure, resilient, and reliable cloud and DevSecOps environments.

The DoD SBIR/STTR process encourages small businesses with innovative ideas to apply to a DoD Component's solicitation. The DoD SBIR program funds approximately $1 billion in grants annually, across 13 DoD Components. The Phase 1 start-up program makes awards up to $150,000 for 6 months and Phase II grants up to $1 million for up to 2 years. During Phase III the idea moves into the marketplace and the small business must find funding in the private sector or through a federal agency. The SBIR program provides opportunities that would be too high risk for venture capital firms to fund. USD(R&E) uses the SBIR process to advance the R&E modernization priorities led by individual principal directors and supported by the Services and COIs.

3.2 Investment in New Approaches to Software Development, Deployment, and Next Generation Management Tools

To keep pace with the rapid rate of innovation and change within the commercial sector, the DoD must fundamentally change its approach to software development, deployment, and application of underlying tools and technologies. The Department must focus on continuous investment in a software S&T approach that enables delivery of new capability to the warfighter through a CI/CD (continuous integration/continuous delivery) process.

The DSSC will review this strategy on an annual basis. In addition, the DSSC, working with the S&T SSG, will develop a detailed implementation plan that focuses on continuous improvement and modernization of the S&T software development and deployment approach, as well as ensuring alignment with latest advances within emerging software tools and technologies.

[53] Nicolas Chaillan, Chief Software Officer, U.S. Air Force, DoD Enterprise DevSecOps Initiative (Software Factory).

The plan will describe a baseline, provide initial recommendations, and define transition metrics to provide feedback that will inform leadership of gaps, lessons learned, and best practices. It will include recommendations to pursue implementation of top investment priorities rapidly while reevaluating the following annually:

- Leveraging universities, laboratories, and FFRDCs to create and maintain a strategic outlook toward software S&T investments, focused on providing rapid curation and continuous evolution of modern, resilient software development capabilities at the speed of relevance.
- Providing rapid access to a variety of out-of-the-box, template-configurable, highly resilient, DevSecOps-based software factories hosted within virtual cloud platform-based environments to streamline start-up and minimize software planning and implementation impacts.
- Leveraging available and existing mature DevSecOps platforms (e.g., Platform One, Black Pearl, CReATE), infrastructure, and resources where possible, to maximize immediate and complete adoption and rapid transformation to modern tools and processes.
- Researching multiple software factory template variants, as needed, to broadly support a variety of project and software capability domains, including enterprise, business, real-time, and cyber-physical.
    - Develop highly secure, reusable software services, components, and capabilities
    - Leverage cloud-native based infrastructure capabilities, software factory, tools, and model-based environments
    - Employ edge computing infrastructure capabilities, MIoT-based sensors, and compute capabilities
    - Provide support for a broad range of domains as needed (e.g., cyber-physical, real-time, C3ISR)
    - Support high-fidelity HWIL and SWIL test and simulation pipeline capabilities
- Considering Air Force examples and other highly successful Agile contracting approaches (i.e., modular contracting, streamlined evaluations) to allow teams to rapidly execute tasks, using short cycle times to continuously provide new and improved iterative capabilities.
- Investing in new deployment approaches leveraging resilient, automated DevSecOps pipelines supporting continuous integration, and continuous delivery from code to deployment.
- Investing in an enterprise-wide software modeling and development ecosystem that integrates tools, with automated build, test, high-fidelity simulation, and delivery pipelines. An integrated framework of shared resources provides the PMO with flexibility to customize configuration with a template-driven approach.
- Employing next generation software management tools. A broad set of modern DoD-viable software development code and project management tools has been evolving over the past decade, largely based on a number of mature Open Source and COTS products (e.g., JIRA,

GitLab, Elastic/Kibana, Grafana). These products are highly extensible and configurable, often requiring the use of plug-ins and additional components to achieve full functionality.

- Reusing software and developing abstraction layers. The implementation of a federated model, data, and software repository will maximize visibility of potentially reusable components across the Department and could lead to major time and cost avoidance. Successful implementation of this reuse may require incentives to intellectual property owners, which may lead to a wider availability of richer, highly mature, and robust reusable models, rich data sets and services. In order to ensure technologies used today can remain relevant and more easily be transferred to programs, avoiding the valley of death, technology abstraction layers will help avoid unnecessary vendor lock-in consistent with Modular Open System Approach (MOSA) objective.
- S&T user-friendly software architecture and designs. S&T software development activities for "black box" systems have typically advanced through a standard approach progressing through throw-away, evolutionary, and incremental prototyping. This process allows rapid transfer of early concepts into immediate code and working capabilities with minimal focus on security, quality, or standards rigor. Future architecture and design considerations must focus on leveraging modern, highly mature cloud platforms (e.g., Platform One, Black Pearl, CReATE), which provides much of the integration, data, and messaging capabilities as a service (e.g., the "undifferentiated heavy lifting"), allowing programs to focus on development of their software applications and the differentiated value it provides. There will be an initial learning curve with regard to development and understanding of the various application templates and archetypes.
- Migrating to cloud computing and microservices. The near future of software, to a large degree, will be focused on cloud-native architectures, distributed terrestrial and space-based edge computing, and sensor networks, largely enabled through ubiquitous connectivity (e.g., 5G, Starlink).

3.3 Ongoing Research and Other Support of Academic, Commercial, and Development Community Efforts to Innovate the Software Development, Engineering, and Testing Process

The key to addressing innovation in software S&T development and reducing software cost and complexity is addressed within the four strategic goals as shown in Table 1 and discussed in sections 2.1-2.4. This approach lays out a multidimensional foundation that focuses on evolving software S&T, addressing many of the gaps/recommendations provided by the FY20 NDAA Section 255 Senior Steering Group, the Services, S&T COIs, DARPA, and other entities involved in this activity. Transformation from the as-is state today to a future state where a software development, engineering, and testing innovation mindset is the norm is the primary goal of this report and recommendations. The solution is not a series of "one and done" activities, but instead the starting point for a cultural evolution, which focuses on a number of ongoing, continuous, and iterative multi-dimensional activities where the whole is greater than the sum of its parts.

The DoD software S&T modernization approach focuses on pervasive automation, inherent integration, and the reduction of complexity for human developers, supporting creation of models and software that are both correct and interoperate with all pieces of large, heterogeneous defense systems. Critical to this approach is early, abundant access to highly resilient, mainstream acquisition technologies, infrastructures, and data through an integrated framework of shared resources (e.g., software, models, data). This approach and the net effect of the combination of the four strategic goals provide the software S&T projects (6.1 basic research, 6.2 applied research, and 6.3 advanced research), create improved parity across the DoD software development realm, and allow a greater potential for early success. This approach also supports the ability for the developed product to more rapidly advance through to R&D and acquisition, supporting rapid fielding and providing an enhanced value to the warfighter and Department.

Many of the recommended software S&T approaches (e.g., MBSE, AI/ML, DevSecOps) are effective in representative commercial environments (e.g., SpaceX, Boeing, Microsoft, Google), but DoD systems with life-critical dependencies to mission operators and ability to address advanced threats (e.g., nation state actors) require an even wider surface area and additional advances to achieve those equities. Given the abundance of highly complex legacy DoD software platforms, the DSSC will work to advance research development of new S&T support approaches, practices, and advanced methods of test and evaluation to support assimilation with modern CI/CD pipelines. This change is challenging and will take time, but needs to be prioritized to the maximum extent practicable if the DoD intends to keep pace with our adversaries.

DoD is increasingly leveraging commercial infrastructure for mission operations, where measuring, assessing, modeling, refactoring, and rapidly redeploying missions on commercial infrastructure are critical. Thus resilient, flexible, and standardized information service architectures are vital for the DoD to maintain and secure its missions so applications can be rapidly developed, deployed, and reconstituted due to disruptions at the physical, cyber, artificial intelligence, or human subcomponent level. This approach is key to both security and resiliency in large complex infrastructures and is important in the context of recent cybersecurity methods such as zero trust architectures.

Finally, key to reducing software cost and complexity is the ability to automate the software lifecycle. Inherent in this process is the reduction of complexity for human developers, allowing development of high quality software that is interoperable with all the pieces of large heterogeneous defense systems. Thus, methods that introduce system modeling and model-based software engineering into the automated DevSecOps process are critical.

Following are the four strategic goals as identified in section 2, figure 1, along with S&T 6.1, 6.2 and 6.3 activity examples as illustrated in Figure 7.

(1) Shifting engineering and software development left starts with iterative enhancement and continuous improvement within the S&T ecosystems to include pervasive automation, use of DevSecOps, enhanced use of modeling and simulation, AI and ML, engineering rigor, a deeper focus on assurance, and early mitigation of technical debt. This strategic goal is the

dependency, or starting point to enable higher parity between S&T and acquisition (Strategic Goal 4), to the maximum extent practicable.

The use of DevSecOps under a Lean Agile approach and highly automated CI/CD pipelines coupled with creation and curation of HWIL/SWIL testing, paired with robust modeling and simulation will allow test and cybersecurity activities to be shifted to the left early, and continuously evaluated across the software development and engineering lifecycle. Further details on Strategic Goal 1 can be found in section 2.1.

- *6.1 – Basic Research Example*: Under fundamental research, the area of model checking has remained a critical area to address design and development of software systems all the way to run time and operations. Model checking requires assessment of whether a model or representation of the logical state of software conforms to a set of properties or structure for correct behavior. Such approaches have been limited to small code bases due to the computational complexity of the process. In recent years, probabilistic or hybrid probabilistic and exact model checking methods have allowed reduction in this computational overhead.
- *6.2 – Applied Research Example*: In the area of applied research, such model checking enables model based systems engineering techniques where analysis of large heterogeneous code bases can be integrated and checked before and during deployment. Such an approach can be used at the source code and binary code level. This approach is critical for design as well as test evaluation of embedded and safety critical systems in order to understand their properties of behavior at runtime and is critical for such systems as flight control in order to guarantee security and performance.
- *6.3 – Advanced Technology Development Example*: With robust methods of model checking and model based software engineering, we now may be able to apply such techniques at the scale required by modern DevSecOps systems. Thus rather than manually updating code and correcting system failures as they occur, we can model critical software functions in advance before software deployment in the DevSecOps environment and then understand the run time properties of the software which needs to be monitored during operation.

(2) The Department does not have an efficient method for sharing available resources, source code, models, and data. This goal will result in a common framework or catalogue, which will support reuse and cost savings by providing visibility to existing S&T capabilities to support S&T and acquisition.

The integrated framework will feature capabilities enabling software S&T, accelerating adoption of modern cloud-native architectures and ecosystems through reuse and ubiquitous access to shared curated environments, models, data, software, tools. The goal is illustrated in section 2.2 within Figure 4.

- *6.1 – Basic Research Example*: In the areas of basic research, a continuous need, particularly in evaluating the performance of machine learning algorithms is the area of risk analysis. Thus the expected performance of a machine learning algorithm is dependent on the data that trains and is processed by the algorithm and the underlying

statistical assumptions of the algorithm itself. Methods such as probabilistic risk analysis evaluate the mismatch between the data entered into the algorithm and the statistical assumptions implicit in the design of the algorithm.

- *6.2 – Applied Research Example*: With advanced risk analysis techniques, the area of verification and validation of machine learning algorithms to include test and evaluation can be developed. In particular, understanding the integrity and security of a particular type of data introduced into a machine learning algorithm is critical, particularly if the algorithm is making life critical decisions. Additionally, maintaining the security of the software supporting the machine learning algorithms itself is also critical.
- *6.3 – Advanced Technology Development Example*: With the preceding research elements, we can now look to processes like the DevSecOps lifecycle itself to support machine learning methods for wide scale software development. Therefore, verification and validation methods for the software supporting machine learning may be advanced to assist in the development of software. Consequently, future ecosystems for software development must leverage machine learning.

(3) Transform the DoD workforce to adopt appropriate technical skills, and a culture to support the Department's modernization vision. Focus on cultivating software engineers, developers, and testers with modern tool set, processes, and capability skills.

To support the ongoing software S&T transition to a Lean Agile culture, leveraging a DevSecOps reference architecture through model-based engineering, APIs, and next generation low or no code software languages, the Department must commit to an ongoing focus on a culture of transformation and creating the workforce of tomorrow.

- *6.1 – Basic Research Example*: In the area of basic research, there have recently been developments in assessment of human developers and user's performance in the integration and use of software. In the software use area, there have been extensive studies of the cognitive performance of cyber operators and this research has been extended to automated training environments. More recently there has been research in the area of the assessment of software developers and their propensity to introduce bugs into code inadvertently during integration.
- *6.2 – Applied Research Example*: In the areas of applied research, methods that assess the risk of users and developers in software use and integration is an emerging research area. Specifically, automated protocols that enforce security guarantees can be structured into the software development pipeline as a function of test and evaluation software pipelines. Additionally, methods that assess the performance of operators and developers as well as automated code generation methods that enforce rigorous guarantees of performance and minimum bugs and security flaws are also critical.
- *6.3 – Advanced Technology Development Example:* As more automated tools in the software pipeline are developed, training the workforce at all levels of technical ability is critical. Online training methods for critical software development are important as well as regular updates for operators and mission users on the latest software resources are important. This training is particularly critical in the context of machine learning software as well as continuous integration and test and evaluation for defense systems.

Partnerships with Defense Universities and academia are critical to maintaining expertise for active duty personnel as well as defense contractors.

(4) Aligning DoD software S&T with acquisition is critical to support the rapid advancement of next generation systems and technologies from S&T into programs of record. The Department's current process of developing black boxes in silos, which then require significant decomposition and rework when transitioning to acquisition, is a major constraint to programs.

The Department requires ongoing research to evaluate the cost, time, efficiency, and other benefits that would result from improving the alignment between software S&T and acquisition.

- *6.1 – Basic Research Example:* Key metrics of assessing the cost and complexity of a software system is the number of interdependencies of systems components on each other and the relative latencies and other system performance metrics that are affected by these interdependencies. Thus methods of assessing these interdependencies stem from model based system representations and mathematical representations such as graph and control theoretic analysis that characterize complex system behavior.
- *6.2 – Applied Research Example:* With this information about system interdependency and complexity, methods in model-based systems engineering have been used recently to influence the acquisition process of software driven systems using predesigned models of system performance before large scale system acquisition. Such systems modeling then can be associated with different cost and development models and plans developed for acquisition of subsystems and then entire system performance specification including technical debt of a variety of system models.
- *6.3 – Advanced Technology Development Example* This pre-modeling approach enables acquisition officers and system designers a means of assessing technical debt as a software system is acquired and the effectiveness in different software solution of meeting acquisition requirements goals. Additionally, this information forms an archive of DoD system design and procurement so models can be exchanged and re-used by contractors in a variety of contexts. This approach is particularly important as information services are consumed and designed in embedded and cloud resourced infrastructures.

3.4 Status of Implementing Recommendations on Software

The Defense Science Board emphasized the importance of the Agile and DevOps commercial practice for robustness and cost reduction in DoD development and infrastructure. The Defense Innovation Board also emphasized the importance of machine learning in the software development and life cycle process and the efficient acquisition mechanisms for more frequent delivery of software to reduce cost and improve interoperability and resilience in software infrastructure.

The NDAA 2019 Section 868 report to Congress summarized the major activities undertaken by the Department to address the recommendations of both the 2018 Defense Science Board report

"Design and Acquisition of Software for Defense Systems" as well as the 2019 Defense Innovation Board report titled "Software Acquisition and Practices." The report outlined 16 initiatives as representative, but not necessarily exhaustive, of the efforts DoD has taken to address the recommendations. The Department published the initial report in early 2018 and has made progress since. The following paragraphs include an updated status of several of the initiatives.

1. Software Acquisition Pathway. The Department released the official software acquisition pathway in October 2020 and is working with the Services for programs to adopt and transition to it. Work remains in refining contract incentives, reporting metrics, and tailoring digital artifacts to accompany the pathway; however, initial reaction to the pathway has been positive.
2. BA-8 Software and Digital Technology Funding. Funding for eight (8) programs was approved to be re-aligned to BA-8 with enactment of FY 2021 Appropriations Act, and these programs have now begun using BA-8. Additional programs were added per Congressional direction to provide baseline data to compare to those not using BA-8. The Department will be able to analyze and assess these activities.
3. DoD DevSecOps Community of Practice. The CoP continues to grow, providing a valuable forum for sharing approaches, lessons learned, best practices, and new technology. The National Institute of Standards and Technology addressed the CoP to update the status and implementation of OSCAL (Open Security Controls Assessment Language) and their experiences supporting FedRAMP.
4. DoD Enterprise DevSecOps Reference Design. This document is undergoing review and being updated to focus on the attributes required for safe and secure DevSecOps programs. The revision will focus on DevSecOps principles and fundamentals with a set of documents describing technical implementations.
5. Defense Security/Cybersecurity Authorization Working (DSAWG) DevSecOps subgroups. These have expanded to 11 subgroups. Some of the subgroups have released their final reports to include guidance on continuous authority to operate, an approach to a cloud-native access point, and security technical implementation guidance (STIG) for container technology and Kubernetes.
6. FY22-26 Capability Programming Guidance. DoD CIO publishes an annual document to provide programming and budgeting guidance of IT investments. This document is used to oversee Department IT budget requests and modernization efforts and provides the basis for the annual certification of Military Department and Defense Agency budgets.
7. Modern Software Metrics. Collaboration with the Practical Software and Systems Measurement Group continues with a focus on defining value assessment metrics for software and programs.
8. Software Workforce Working Group. The working group has made significant progress as reported in the FY20 NDAA Section 862 report delivered to Congress in January 2021. That report outlines an approach to training and development for the software and software acquisition workforce (aka Digital DNA) that DoD is implementing.

The remaining initiatives from the report are either already completed with no more activity to report or have been combined with the above efforts (e.g., DAU DevSecOps Academy is being merged into the efforts of the software workforce working group and the Digital DNA pilot).

3.5 DoD Efforts Supporting Software Acquisition, Technology Development, Testing, Assurance, and Certification

The DoD funds R&D activities through numerous avenues. The Department sponsors research conducted by multiple organizations nationwide, including Science and Technology Reinvention Laboratories, universities, FFRDCs, and Service organizations with activities in software engineering.

FFRDCs are governed by the Federal Acquisition Regulation, Section 35.017, and provide specialized R&D capabilities that cannot be effectively met by the Federal Government or the private sector alone. FFRDCs advise program of record software development and test teams on DevSecOps, and software architectures to enable faster transition of DevSecOps techniques into government and contractor development teams to mitigate deployment and operational risks. This support enables continued widespread adoption of DevSecOps across DoD.

The DoD S&T Reinvention Laboratories are increasingly using modern cloud-based software practices such as DevSecOps. Key to this approach is the ability to integrate across research projects and then transition research effectively to DoD acquisition programs. The U.S. Air Force has already rebranded its software sustainment laboratories to software engineering labs, and is establishing widespread adoption of DevSecOps and their common Platform One ecosystem.

The U.S. Navy has established and is releasing a common development platform called Black Pearl, an instantiation of Platform One, but more applicable to the Navy. The U.S. Army Futures Command and PEO Enterprise Information Systems recently started their journey to establish DevSecOps environments at their software sustainment (development) centers. In addition, Army Futures Command launched the Army's first software factory, dedicated to soldier-led software development utilizing shared IaaS and PaaS offerings to deliver valuable software to soldiers worldwide. Research activities in DARPA continue to fill gaps rapidly and affordably. DARPA has leveraged cloud-computing capabilities to access mission data provided by the Services and to facilitate the deployment of new technologies.

In the near future, DARPA R&D will produce new technologies that will readily deploy on the Platform One environment to support mission needs. DARPA is continuing to develop advanced software design and analysis technologies to include some of following initiatives; Automated Rapid Certification of Software Program (ARCOS), Cyber Assured Systems Engineering Program (CASE), High Assurance Cyber Military Systems Program (HACMS), Intent-Defined Adaptive Software (IDAS). Acquisition programs of record need to be aware of these capabilities, pulling them into their systems if needed by adopting a common ecosystem and shifting engineering left to accelerate the transition of these type of advanced R&D capabilities.

The Test Resource Management Center (TRMC) ensures the readiness and modernization of the DoD T&E infrastructure and workforce through governance and sustainment of the Major Range and Test Facility Base (MRTFB), which consists of 23 test ranges. The TRMC investment program initiates technology development for DoD T&E infrastructure and provides early forecasting of test technology needs while collaborating with the S&T community.

3.6 Transition of Relevant Capabilities and Technologies to Programs

The strategic vision, goals, and focus areas all support the most important software R&D goal, the transition of new capabilities to weapon systems and funded programs of record. A unified plan for exchange of software products and innovation within the DoD as well as the commercial sector is critical to maintaining technical superiority for DoD missions involving software.

Ongoing work in the Army, Navy, and Air Force, as well as the Office of the DoD CIO and OUSD(A&S), is enabling a mix of DoD and commercial cloud infrastructure to receive the rapid pipeline of software emerging from the new DoD DevSecOps software environment. It is critical to enable tight collaboration between low TRL research all the way to high TRL prototyping and development. Transition time between these domains can be as short as months in this new environment.

For transitioning relevant software capabilities and technology from S&T to acquisition programs of record, the S&T strategy focuses on the following initiatives:

1. A federated view of S&T activities across the Department including sufficient detail on supporting system domain (e.g., real-time, cyber-physical, C3ISR, mission planning, business system) and other pertinent attributes about the software architecture, heritage, languages, etc.
2. Department-wide unified S&T transition plan to define standards, processes, and activities necessary to support a more seamless transition from S&T to the programs. The plan will address visibility, coordination, reuse, software architecture approach, cybersecurity, and quality standards.
3. Metrics to inform leadership on transition effectiveness and plan adoption across the Department.

4 Next Steps

This Department-wide software S&T strategy provides a way forward, but with the pace of change the software S&T strategy cannot remain static. The DSSC (currently OUSD(R&E) Engineering) will continue working with the FY20 NDAA Section 255 SSG, S&T COIs, DARPA, CIO, FFRDCs, and other DoD software experts to advance the following activities.

1. Establish software S&T modernization governance to create and coordinate detailed implementation planning, and to implement and monitor transformation metrics to provide a feedback loop.
    a. Software S&T modernization governance will focus on creation of a highly responsive, rapid, and iterative operations tempo, user, and stakeholder collaboration. This will facilitate continuous feedback loops, ensuring decisions are better aligned with users, stakeholders, and the Department's needs.
2. Establish a DevSecOps software factory within appropriate enterprise infrastructure (e.g., Platform One, Blackpearl, CReATE, on-premise, hybrid).
    a. Services and agencies can leverage this strategy to develop plans to integrate S&T programs across basic, applied and advanced research projects.
    b. The DSSC will facilitate focus on use of DevSecOps resources to deliver more benefits that are common across S&T.
3. Focus on workforce training across Agile program management, Agile software development tools and techniques, and the DevSecOps ecosystem.
4. Revise contract requirements:
    a. Support software development within Government-owned environments (e.g., software factory) where appropriate.
    b. All software is to be managed, including software development licenses and tools required to compile, test, validate, integrate, deploy, operate and monitor software, via automated continuous integration and continuous delivery pipelines.
5. Work with the Services to continually refine and update this strategy based on forward-looking mission needs, leveraging DoD wide S&T to deliver benefit jointly.
6. Review the strategy annually.

Appendix A: Section 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).

Acronyms

AI/ML	artificial intelligence/machine learning
API	application programming interface
ARCOS	Automated Rapid Certification of Software Program
A&S	Acquisition and Sustainment
ATO	authority to operate
CASE	Cyber Assured Systems Engineering Program
cATO	Continuous Authority to Operate
CD	continuous deployment
CI	continuous integration
CIO	Chief Information Officer
COI	community of interest
COTS	commercial off-the-shelf
CReATE	Army Code Repositories and Transformation Environment
DARPA	Defense Advanced Research Projects Agency
DAU	Defense Acquisition University
DevSecOps	Development, Security, Operations
DHA	Direct Hire Authority
DISC	Digital Integration Support Cell
DoD	Department of Defense
DOT&E	Director of Operational Test and Evaluation
DWP	Digital Warfighting Platform
ECMA	Enterprise Cloud Management Agency
EHA	Expedited Hire Authority
EMD	Engineering and Manufacturing Development
FaaS	Function as a Service aka Serverless
FFRDC	Federally Funded Research and Development Centers
HACMS	High Assurance Cyber Military Systems Program

HWIL	hardware-in-the-loop
IDAS	Intent-Defined Adaptive Software
JAIC	Joint Artificial Intelligence Center (JAIC)
MBSE	model-based software engineering
MBSE	model-based systems engineering
MDA	Missile Defense Agency
MIoT	Military Internet of Things
MRTFB	Major Range and Test Facility Base
NDAA	National Defense Authorization Act
NDS	National Defense Strategy
OJT	on the job training
OPM	The Office of Personnel and Management
POR	Program of Record
R&D	research and development
RPA	Robotic Process Automation
SBIR	small business innovative research
SETA	Systems Engineering Technical Assistance
SME	subject matter expert
SOFAC	Software Factory Platform
S&T	science and technology
SWIL	software-in-the-loop
T&E	Test and Evaluation
TMRR	technology maturation and risk reduction
TRL	Technology Readiness Level
TRMC	Test Resource Management Center
USD(R&E)	Under Secretary of Defense for Research and Engineering
ZTA	zero trust architecture

Acknowledgments

The following DoD senior steering group (SSG) members provided significant contributions to this strategy. The SSG is group of software subject matter experts convened to review the congressional language and inform the development of this strategy. The SSG members and significant contributors include:

- OUSD(R&E) sponsor and study lead: Mr. Timothy Dare and Mr. Allan Dianic
- OUSD(R&E): Dr. Jill Crisman, Dr. Robert Bonneau, Dr. Daniel Ragsdale, Mr. George Rumford
- OUSD(A&S): Dr. Jeff Boleng and Mr. Sean Brady
- DoD CIO: Mr. Rob Vietmeyer, Mr. Dan Risacher, Mr. Tom Morton, Mr. Peter Ranks, Mr. Jason Weiss
- DOT&E: Dr. Amy Henninger
- U.S. Air Force: Mr. Nicolas Chaillan, Ms. Hannah Hunt
- U.S. Navy: Mr. Richard Jack
- U.S Army: Mr. Leo Garciga, Mr. Paul Puckett
- Technical writing: Mr. M. Timothy Stark and Mr. Jerry Tarasek, OUSD(R&E)/Engineering

Department of Defense Software Science and Technology Strategy

Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301