Report to Congress
on
Implementation of Defense Science Board Report Recommendations, "Design and Acquisition of Software for Defense Systems"
Section 868 of the National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232)

Office of the Under Secretary of Defense For Acquisition and Sustainment

The estimated cost of this report or study for the Department of Defense is approximately $17,000 in Fiscal Years 2019 - 2020. This includes $5,000 in expenses and $12,000 in DoD labor.

Generated on 2020Apr16 RefID: D-EC0F53C

This page intentionally left blank.

Executive Summary

As required by section 868(c) of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (P.L. 115-232), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) herewith provides this summary report of initiatives and actions that have been implemented in response to the February 2018 Defense Science Board Report titled "Design and Acquisition of Software for Defense Systems."

After receiving the DSB report in February 2018, the department also collaborated with the Defense Innovation Board (DIB) on the Software Acquisition and Practices (SWAP) study, as required in NDAA 2018 Section 872. The DIB SWAP study was delivered to Congress in May 2019. Since that delivery, OUSD(A&S) in collaboration with various other OSD Directors (namely R&E, CIO, P&R, Comptroller, CAPE, and DOT&E) has been aggressively pursuing implementation of both the DSB and DIB SWAP recommendations. This report details the significant initiatives, activities, and progress that have been made by DoD toward modernizing the software development capabilities of the Department.

The following table summarizes the major key initiatives that have resulted from both the 2018 Defense Science Board Study and the 2019 Defense Innovation Board Study and how they address the DSB recommendations.

		DSB Recommendation						
	Initiative	1	2	3	4	5	6	7
1	Software Acquisition Pathway		X		X		X	
2	BA-8 Software and Digital Technology Funding		X		X			
3	DoD DevSecOps Community of Practice	X	X		X			
4	DoD Enterprise DevSecOps Reference Design	X	X		X			
5	DSAWG DevSecOps subgroups		X	X	X			
6	FY22-26 Capability Programming Guidance		X	X	X			
7	Modern Software Metrics	X	X	X				
8	Software Workforce Working Group					X		
9	Key Leadership Position in Programs for Software					X		
10	Define and Create Modern Software Career Field(s)					X		
11	USAF Creation of 16K (officer) and 8K (enlisted) career fields					X		
12	DAU DevSecOps Academy and RAND Report		X			X		
13	DoD Enterprise DevSecOps Services (Platform1, Repo1, IronBank, etc.)		X				X	
14	Artificial Intelligence Executive Steering Group Test and Evaluation Committee							X
15	DOT&E AI and Autonomous Systems Test and Evaluation Steering Group							X
16	DDR&E Cornerstone Prototype							X

Table of Contents

1 Overview

As required by section 868(c) of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (P.L. 115-232), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) herewith provides this summary report of initiatives and actions that have been implemented in response to the February 2018 Defense Science Board Report titled "Design and Acquisition of Software for Defense Systems." Section 868 is included as Appendix A for reference.

In most cases the recommendations tasked OUSD(R&E) and various other agencies with action. After receiving the DSB report in February 2018, the department also collaborated with the Defense Innovation Board (DIB) on the Software Acquisition and Practices (SWAP) study (as required in NDAA 2018 Section 872), which was delivered to Congress in May 2019. Since that delivery, OUSD(A&S) in collaboration with various other OSD Directors (namely R&E, CIO, P&R, Comptroller, CAPE, and DOT&E) has been aggressively pursuing implementation of both the DSB and DIB SWAP recommendations. Below are the significant initiatives, activities, and progress that have been made by DoD toward modernizing the software development capabilities of the Department, the Defense Industrial Base, and the non-traditional vendor communities and tech-sector. Included in each case is a discussion of how these accomplishments relate to the implementation of the seven DSB recommendations, which are included as Appendix B.

2 Implementation of Modern Software Development Acquisition Policy

2.1 Software Acquisition Pathway

On January 3, 2020, OUSD(A&S) released interim acquisition policy creating the new Software Acquisition Pathway. The policy memorandum and pathway details are accessible here:

- https://www.acq.osd.mil/ae/assets/docs/USA002825-19%20Signed%20Memo%20(Software).pdf.

Both are included as Appendix C. This policy is a component of the Adaptive Acquisition Framework (https://aaf.dau.edu/), which has been a major focus of OUSD(A&S) to modernize not just the Department's approach to software acquisition, but modern capability acquisition generally. This policy is released as Interim Acquisition Guidance specifically so feedback and learning can be gathered as programs adopt the pathway. Based on this feedback and lessons learned, final policy guidance will be published by the end of 2020 in an approach similar to that used for the development of DODI 5000.80, Middle Tier of Acquisition. These actions directly address **DSB recommendation 2** advising the department to adopt continuous iterative development. Additionally, this addresses **DSB recommendation 4**, by empowering the Services, PEOs, and PMs to immediately adopt a modern approach to software development in ongoing and new acquisition programs.

2.2 Software and Digital Technology Funding

In addition to the development and release of the Software Acquisition Policy, the Department has pursued several other initiatives. First is the ongoing successful execution of a number of

Agile Software pilot programs as directed in NDAA 2018 Sections 873 and 874. Progress reports on those efforts have been previously delivered to Congress.

Multiple 873 and 874 programs have proposed that software acquisition would be supported more effectively through the use of a single funding category for software and digital technology. This echoes a major recommendation of the Defense Innovation Board in the SWAP report and stands to directly support **DSB recommendations 2 and 4**. As a result, OSD is working with the Comptroller on another significant pathfinder program for the creation of Budget Activity 8 (BA-8) under the Research, Technology Development, and Engineering (RTD&E) title. In FY-21 DoD is seeking congressional approval to consolidate funding for a small number of on-going programs under a single "color" of money for software and digital technology. This pilot effort will evaluate the efficacy of a single funding category for software and digital technology.

2.3 DSAWG Subgroups and Authority to Operate

Additional policy initiatives supporting the DSB and DIB recommendations (specifically **recommendations 2, 3, and 4**) are being implemented by the DoD CIO in support of the DevSecOps Community of Practice, which is discussed in section 3. These include the creation of seven subgroups by the DISN Security Accreditation Working Group (DSAWG). These seven subgroups are focused on updating cyber security and accreditation policy and practices in the following areas:

1. Continuous update and maintenance of the DoD DevSecOps Reference Design,
2. Establishing a Kubernetes Security Requirements Guide (SRG),
3. Establishing a container SRG,
4. Designing, implementing, prototyping, and evaluating a DevSecOps Access Point for secure multi-factor access to Impact Level 4 and 5 cloud instances by industry partners,
5. Collaboration with the National Institute of Standards (NIST) to develop a Government wide NIST DevSecOps Reference Design,
6. Define, establish, and publish continuous Authority to Operate (cATO) guidance in support of DevSecOps for pipelines, tools, teams, with required deliverables/artifacts, and
7. Establish the required training for Security Controls Assessors (SCAs), Information Systems Security Managers (ISSMs), and Approving Officials (AOs) to implement and adopt cATO policy.

2.4 Capability Programming Guidance for FY2022-2026

The DoD CIO is also including language in its Capability Programming Guidance for Fiscal Years 2022-2026 requiring the Military Services to program funds to support DevSecOps practices for new software development efforts. The goal is to realize use of DevSecOps practices by 95% of new software efforts by FY2026. The specific guidance includes the following (paragraph numbers are from the quoted source document):

> (U//FOUO) 4.2.1 DevSecOps Use Enabling Infrastructure Capabilities. Army, Navy, Air Force, and Marine Corps resource in FY2022 and through the FYDP infrastructure activities necessary to enable the use of DevSecOps practices by 95% of all new software development efforts by FY 2026 consistent with DoD acquisition policies.

U//FOUO) 4.2.2 DevSecOps Training/Skills Development. Army, Navy, Air Force, and Marine Corps resource in FY2022 and through the FYDP the appropriate training and skills development initiatives to enable use of DevSecOps practices by 95% of all new software development efforts by FY 2026.

(U//FOUO) 4.2.3 DevSecOps Visibility and Reporting. Army, Navy, Air Force, and Marine Corps resource a capability to enable the visibility and reporting of new software development efforts, DevSecOps adoption, and DevSecOps metrics such as deployment frequency, lead time for changes, change failure rate, and time to restore service.

3 Department wide DevSecOps Community of Practice (CoP) and Enterprise Services

In 2018 the Department founded the DevSecOps Community of Practice (CoP) (https://www.milsuite.mil/book/groups/dod-enterprise-devsecops). Since its founding, the community has grown to include hundreds of members from all Services and DoD Support Agencies. This CoP meets regularly for sharing information and best practices. The CoP is guided by Senior Steering Group from DoD, A&S, CIO, DDS, DISA, and the Services (led by the AF Office of the Chief Software Officer, CSO) which meets bi-weekly.

3.1 DoD Enterprise DevSecOps Reference Design

This collaboration led directly to the development and publication of the DoD Enterprise DevSecOps Reference Design (https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583) in August 2019 which is included as Appendix D. Significantly, this reference design was endorsed jointly by the DoD CIO and OUSD(A&S) in the memorandum attached as Appendix E as the preferred approach to DoD software development. This action directly addresses **DSB recommendations 1, 2, and 4**. It creates a reference design for program managers to directly assess agencies' and vendors' software factories, as well as emphasizing that DevSecOps is the preferred approach to DoD software development and acquisition. The reference design provides detailed and concrete guidance to new and existing programs.

3.2 Establishment of Enterprise Services

Perhaps even more significantly, this effort has led directly to the creation of Enterprise DevSecOps capabilities and services that are available to all acquisition programs. The pathfinder for this effort is the Air Force's office of the Chief Software Officer (CSO). More information is available here: https://software.af.mil/ and here: https://software.af.mil/dsop/. The DoD CIO and DISA are working closely with the DevSecOps CoP and Senior Steering Group to move AF solutions to enterprise scale offerings leveraging both the AF efforts with Cloud One and Platform One to bring the same capabilities to the DoD's JEDI effort when possible.

A complete list of emerging DevSecOps services that have been established is available here: https://software.af.mil/dsop/services/. Examples include:

- a DoD Centralized Container Source Code Repository (DCCSCR - https://repo1.dsop.io),
- a DoD Centralized Artifact Repository (DCAR/Iron Bank - https://ironbank.dsop.io/),
- Platform One – reference implementation of the DevSecOps reference design,
- DevSecOps Basic Ordering Agreements for DevSecOps tools, services, and talent, and
- DevSecOps Access Point to virtualize secure access to program DevSecOps development and operations cloud instances.

4 Measuring Software Development Effectiveness

In order to directly address the **DSB Recommendation 3**, DoD has been working closely with industry associations to ensure metrics and consequently contract performance incentives are collaboratively defined. This work also directly supports **DSB Recommendation 1**. Collaboration with the National Defense Industry Association (NDIA - https://www.ndia.org/, reference https://www.ndia.org/divisions/systems-engineering/studies-and-publications) and the Practical Software Measurement group (http://www.psmsc.com/), has resulted in a comprehensive set of metrics to evaluate both vendor software factories and delivered software usefulness. The definitive work of this collaboration, the Continuous Iterative Development Measurement Framework, is available here: http://www.psmsc.com/Downloads/CIDProducts/CID%20Measurement%20Framework%20-%20v1-0.pdf and is included as Appendix F. Figure 1, which is taken from that report, summarizes the defined metrics for modern software development.

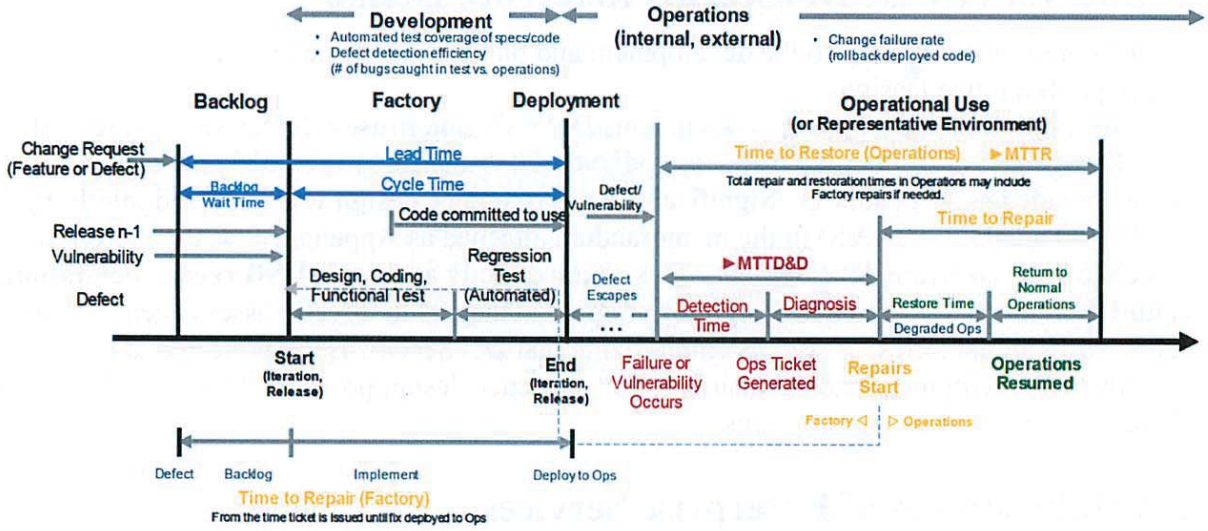

Figure 1 – Modern Software Development Metrics

5 Workforce Initiatives

In order to directly address DSB **Recommendation 5**, OUSD(A&S) created the software workforce working group which enjoys membership from all Services and OSD Directorate representatives from P&R, R&E, CIO, DDS, and A&S.

5.1 Establishment of Key Leader Position and Software Career Field Modernization

Significant efforts that have already been initiated by this working group include the legislative proposal to ensure software intensive programs define a key leadership position for major acquisition programs for a software architect as an inherently governmental position. Other efforts include collaborating with multiple other governmental organizations to work with OPM on the creation of a modern software development civilian career field. Representative of other significant initiatives are the establishment of the 16K Officer career field and the 8K Enlisted career field specifically for software development professionals by the USAF.

5.2 Defense Acquisition University

Further efforts responding to **DSB Recommendation 5** are evidenced by the continuous improvement and adaptation by Defense Acquisition University (DAU) in response to stakeholder requests and Acquisition Professional demand signals. Over the last two years, DAU has hired multiple Agile and DevSecOps professionals, in addition to developing course work and acquiring commercially available best in class courseware to educate and empower the acquisition workforce. Much more detail of the progressive actions of DAU can be explored here: https://www.dau.edu/cop/it/Pages/Topics/DevSecOps.aspx. Additionally, Appendix H has expanded detailed information about DAU's Software Acquisition Management Curriculum.

As part of the workforce development initiative, R&E tasked the RAND Corporation, a Federally Funded Research and Development Center, to investigate three areas to help improve the ability of the DoD software acquisition workforce to more 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 training. Third was to recommend options for tracking and managing a software acquisition workforce. The full report is provided as Appendix I. The DAU DevSecOps Academy Workshops have rapidly filled training and education gaps identified in the report.

6 Software is Continuously Engineered and Developed, not "Sustained"

Implementation of **DSB Recommendation 6** is being accomplished by the implementation and adoption of DoD Enterprise DevSecOps services and cloud instances (reference Section 3.2 above). Emerging best practice to ensure appropriate government access to all required software development artifacts (e.g. code, configuration scripts, test scripts, scanners, compilers, tools) is being accomplished by establishing and providing government owned and operated cloud development environment for all contributing parties in which development and integration can

be performed. This emphasizes Government Ownership and proper marking from "birth" and enables cooperative development by both industry and organic personnel throughout the life of the software.

6.1 Examples of DevSecOps Best Practices

This approach is exemplified by the Air Force's Kessel Run (KR) Development unit (AFLCMC Detachment 12). Combined government and contractor teams have established a DevSecOps infrastructure in GovCloud called Kessel Run Enterprise Services (KRES). This environment includes all necessary software development, security scanning and enforcement, testing, fielding, operations, and operational monitoring services and infrastructure to enable software development teams to move fast and start iterating with user's on day 1. This environment is provided to contributing teams (government and contractor) as Government Furnished Equipment (GFE) and all software digital artifacts are hosted and stored in this GFE environment. Care is taken to include appropriate safeguards and delivery mechanisms for those instances containing contractor proprietary information. Since all digital artifacts are created, integrated, tested, fielded, and operated in a government provided cloud instance, delivery and appropriate access are inherently provided. This best practice is being adopted by numerous other major programs as a result of the success seen by KR and the AOC Pathfinder effort. Notable programs adopting this approach are the Joint Strike Fighter Program (JSF), Ground Based Strategic Deterrent (GBSD), Unified Platform (UP), and the Naval Operational Business Logistics Enterprise (NOBLE).

7 Independent Verification and Validation for Machine Learning

7.1 Artificial Intelligence Executive Steering Group

With leadership from the Joint Artificial Intelligence Center (JAIC), the DoD CIO established the Artificial Intelligence (AI) Executive Steering Group (ESG) (reference Appendix G), which includes a working group dedicated to AI Test and Evaluation. The key tasks this group is addressing are:

- Create the methods and mechanisms to drive the establishment of Department-wide standards and practices for test and evaluation of AI models, supporting data, and AI-enabled technologies during development, integration, and deployment in production and operational environments.
- Develop the process for identifying AI T&E gaps and integrate funding of AI Test Technology and Infrastructure into the current DoD Test Infrastructure process.

Additionally, the Director of Operational Test and Evaluation (DOT&E) has also established a supporting effort known as the Artificial Intelligence (AI) and Autonomous Systems (AS) Test and Evaluation Steering Group.

7.2 DDR&E Cornerstone Prototype

Concrete progress has been made by a prototype effort called Cornerstone. Cornerstone is an OSD DoD Defense Research and Engineering (DDR&E) funded collaborative project between

the UK's Defense Science and Technology Laboratory (dstl), Combatting Terrorism Technical Support Office (CTTSO), DTRA, and USD(R&E). The four major goals of Cornerstone are to: 1) increase the USG's foundational knowledge and situational awareness within the Chem-Bio domain; 2) facilitate real-time information sharing and collaboration between DTRA and foreign partners; 3) conduct fully automated verification and validation (V&V) of operational analytical tools; and 4) establish a framework that will accelerate the Artificial Intelligence (AI) DevSecOps engineering lifecycle.

Cornerstone's frameworks for both V&V and DevSecOps are flexible and adaptable to different problem domains, data sources, and algorithms employed. The V&V framework in Cornerstone can compare the outputs from multiple concurrent machine learning models with ground truth provided by analysts and other heuristic indicators. This framework enabled analysts to provide instant feedback on situations where natural language processing pipelines were challenged, and the developers were able to address these issues in rapid fashion.

(U//FOUO) In January 2020 a DTRA/dstl bilateral exercise was conducted via the Cornerstone framework. During this exercise a DTRA biology WMD expert was able to characterize 17 historical disease outbreaks, discover 13 new biological facilities of interest, and identify 122 novel pathogens stored in a specific geographical region—this represents a four-fold increase in the analyst's productivity. The exercise demonstrated the effectiveness of the Cornerstone V&V framework.

8 Summary

The following table summarizes the major key initiatives that have resulted from both the 2018 Defense Science Board Study and the 2019 Defense Innovation Board Study.

	Initiative	DSB Recommendation 1	2	3	4	5	6	7
1	Software Acquisition Pathway		X		X		X	
2	BA-8 Software and Digital Technology Funding		X		X			
3	DoD DevSecOps Community of Practice	X	X		X			
4	DoD Enterprise DevSecOps Reference Design	X	X		X			
5	DSAWG DevSecOps subgroups		X	X	X			
6	FY22-26 Capability Programming Guidance		X	X	X			
7	Modern Software Metrics	X	X	X				
8	Software Workforce Working Group					X		
9	Key Leadership Position in Programs for Software					X		
10	Define and Create Modern Software Career Field(s)					X		
11	USAF Creation of 16K (officer) and 8K (enlisted) career fields					X		
12	DAU DevSecOps Academy and RAND Report		X			X		
13	DoD Enterprise DevSecOps Services (Platform1, Repo1, IronBank, etc.)		X				X	
14	Artificial Intelligence Executive Steering Group Test and Evaluation Committee							X
15	DOT&E AI and Autonomous Systems Test and Evaluation Steering Group							X
16	DDR&E Cornerstone Prototype							X

9 Included Appendices

Appendix A – NDAA 2019 Section 868

Appendix B – Defense Science Board Software Report Recommendations

Appendix C – Software Acquisition Pathway

Appendix D – DoD Enterprise DevSecOps Reference Design

Appendix E – Endorsement memo of DoD Enterprise DevSecOps Reference Design

Appendix F – Practical Software and Systems Measurement Continuous Iterative Development Measurement Framework

Appendix G – DoD Artificial Intelligence Executive Steering Group Memorandum

Appendix H – DAU Software Acquisition Management Curriculum

Appendix I – Software Acquisition Workforce Initiative, Initial Competency Dev (RAND Report)