DoD Enterprise DevSecOps Change Log

September 2021

Document Set Version 2.1

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Overview

The transition from a DevSecOps document (singular) to a DevSecOps document set was intended to provide a stable strategy and set of fundamentals while enabling refinement to the tools, activities, reference designs, and playbook plays at the speed of relevance. The rolling change log below captures the modifications made to each document within the document set.

Pathway to a Reference Design

Community proposed reference designs need to be evaluated in a transparent and consistent manner. The DoD Enterprise DevSecOps Reference Design Pathway document outlines the journey from community proposal to approved reference design.

Automatic Expiration

Several documents in the set now include a new call out on the cover page to indicate that they automatically expire one (1) year from the publication date. This recognizes and addresses two distinct problems. First, as Distribution A documents that are cleared for public release, there is no way to recall or control the distribution of the PDF files once approved and published. The wide dissemination of these publicly released documents has led to stale and outdated versions being circulated, and adding the automatic expiration date ensures that any reader regardless of how they obtained the PDF is informed that they may be consuming a stale or dated version of the document.

Second, the inclusion of an automatic expiration date recognizes the speed at which industry and software development activities transform. What was considered a best practice yesterday may not be considered a best practice tomorrow. Automatic expiration serves as a triggering function to review the materials in these documents on a regular cadence to ensure relevance and alignment with industry recognized best practices.

The affected documents will include a banner like this on their cover page:

This document automatically expires 1-year from publication date unless revised.

The documents affected include:

- DevSecOps Tools and Activities Guidebook
- DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes
- DRAFT DoD Enterprise DevSecOps Reference Design: AWS Managed Services
- DRAFT DoD Enterprise DevSecOps Reference Design: Multi-Cluster Kubernetes
- Playbook – DevSecOps

Doc Set Version	Document	Document Version	Section	Change
2.1	**Reference Design Pathway**	1.0		*Initial Release*
	Strategy	2.1	*Headings*	Numbered headings have been applied to the document for easier reference in conversation to a specific part of the strategy.
			Page Numbering	Proper page numbering applied, with i, ii, … for front matter and 1, 2, … for main body of document.
			5. Formal Recognition of the Supply Chain	The use of the product rule has been clarified to be *illustratively* used, since it is not feasible to quantitatively calculate the precise cybersecurity level of a software product.
			9. DevSecOps Management and Governance	Included appropriate references to DT&E in addition to OT&E.
			Figures (Multiple)	Figures updated their cross-hatch pattern to print better on monochrome printers.
			Figure 3	Clarification made in the text that the cybersecurity activities in the outer rim are **notional** and do not represent a complete set of activities undertaken by a team due to spacing limitations.
			Figure 7	Clarification that the listed tests are notional and represent an incomplete list of tests that would actually be performed at a control gate.
	Fundamentals	2.1	*Headings*	Numbered headings have been applied to the document for easier reference in conversation to a specific part of the strategy.
			Page Numbering	Proper page numbering applied, with i, ii, … for front matter and 1, 2, … for main body of document.
			Multiple	Pattern used for identification of specific cyber security aspects in the various graphics has been updated to print better when using a grayscale printer.
			Figures (Multiple)	Multiple figures updated their cybersecurity cross-hatch pattern to print better on monochrome printers.

			4.1 DevSecOps Overview	Clarification made in the text near figure 4 that the cybersecurity activities in the outer rim are **notional** and do not represent a complete set of activities undertaken by a team due to spacing limitations, and that readers should review the DevSecOps Tools and Activities Guidebook for a complete set of required/preferred activities.
			5.2 Importance of the DevSecOps Sprint Plan Phase	Incorporated qualifications regarding story- or epic-level activities. Also qualified the references to Minimum Viable Product and Minimum Viable Capability Release as stated in DoDI 5000.87.
			Figure 6	Clarification that the listed tests are notional and represent an incomplete list of tests that would actually be performed at a control gate.
			Figure 14	‘Why Interconnect’ explanation has been added to expand upon how that phrase came to be used.
			6. DevSecOps Platform & Figure 14	Clarification that the *Interconnect* concept is used both within and at the boundaries of any given layer to define a reference design’s unique set of tools and activities. It is intended to identify something that connects two different things together; it is **not** intended to be interpreted as a network interconnect.
			7. Current and Envisioned DevSecOps Software Factory Reference Designs	Updated this section to reflect additional **draft** reference design released. Language indicating that the CNCF K8s reference design was the sole approved reference design has been stricken in anticipation of future approved reference designs, but **the document acknowledges that the CNCF K8s reference design remains the most mature reference design available to DoD**.
			8. Deployment Types	Relocated the Deployment Types section, to include blue/green deployments, canary deployments, and rolling deployments, and continuous deployments out of the K8s Reference Design into the Fundamentals. These concepts are equally applicable across multiple reference designs.

			Multiple	Included appropriate references to DT&E in addition to OT&E, including an update to Figure 7.
			Multiple	Routine typographical errors fixed.
			Acronyms Table	Removed several unused and irrelevant acronyms.
	Tools and Activities Guidebook	2.1	*Headings*	Numbered headings have been applied to the document for easier reference in conversation to a specific part of the strategy.
			Page Numbering	Proper page numbering applied, with i, ii, … for front matter and 1, 2, … for main body of document.
			2.2 Plan Tools and Activities	Qualified software development *activities*.
			Table 3	Removed reference under “Asset inventory management” to “Collect information about all IT assets,” as that would occur at the organizational level.
			Table 3	Configuration management tooling is REQUIRED
			Table 4	Added a new row for “Requirements database” at the PREFERRED level.
			Table 6	Application, Infrastructure, and Security code development activities have been updated to reflect an expectation that source code should be accompanied by unit, integration, etc. tests as input and test results as output.
			2.5 Test Tools and Activities	Clarification that testing “focuses on how the system supports the mission.”
			2.5 Test Tools and Activities	Added “Production stage” to the bullet list, joining the existing development, system, and pre-production stage bullets.
			Table 10	Added single row to capture both DT and OT activities
			Table 12	DT and OT activities were moved from Table 12, Release and Deliver Phase Activities, to their correct location in Table 10, Test Phase Activities.
			Table 14	Added OT&E activity
			Table 16	Qualification that ‘Feedback’ may include additional OT&E activities

			Table 17	Clarification: InfoSec Continuous Monitoring (ISCM) **Tool**.
			Table 17	Clarification: Cyber Threat **Intelligence Subscription**.
	DevSecOps Playbook	2.1	*Cover Page*	Simplified the title to simply "DevSecOps Playbook"
			Play 10	Expanded to include all test and evaluation activities, both DT&E and OT&E.
			Play 11	Industry Contribution
	CNCF Kubernetes Reference Design	2.1	*Page Numbering*	Proper page numbering applied, with i, ii, … for front matter and 1, 2, … for main body of document.
			1.2 Purpose	Emphasis has been added that the software container is the standard unit of deployment in this reference design, that software factory produces applications and application artifacts as a product, and that K8s is expected in the production environment when using this reference design.
			** Deployment Types*	Relocated the Deployment Types section, to include blue/green deployments, canary deployments, rolling deployments, and continuous deployments out of the K8s Reference Design into the Fundamentals. These concepts are equally applicable across multiple reference designs.
			Tables (Multiple)	Fixed inconsistency between Tools & Activities Guide and Reference Design to use REQUIRED and PREFERRED. Previous entries that were listed as RECOMMENDED in 2.0 have been updated for consistency to read PREFERRED.
			Figures (Multiple)	Multiple figures updated their cybersecurity cross-hatch pattern to print better on monochrome printers.
			3. Software Factory Interconnects, and Figure 1	Clarification that the *Interconnect* concept is used both within and at the boundaries of any given layer to define a reference design's unique set of tools and activities. It is intended to identify something that connects two different things together; it is **not** intended to be interpreted as a network interconnect.

			Table 1, 8, & 14	Removed reference to Security Content Automation Protocol (SCAP) and replaced with the requirement for a structured machine-readable format.
			Table 1	Service Mesh and Service Mesh Proxy has been clarified as REQUIRED only if the application uses microservices.
			Table 1	The 'Artifact Repository' row did not relate to the SCSS and was removed from this specific table.
			4. Software Factory K8s Reference Design	Restructured the first paragraph's second sentence to simply refer to Iron Bank; there is no document in this document set entitled "DoD Enterprise DevSecOps Container Service."
			4. Software Factory K8s Reference Design	The SCSS monitors the application, not the factory. This mistake has been fixed in paragraph 2 of this section.
			4. Software Factory K8s Reference Design	Clarification that the software artifact, not the pipeline, moves between stages.
			Table 2	Table was incorrectly labeled CD/CD and has been fixed to properly read CI/CD; removed the first column which was fully redundant since the entire table describes CI/CD features, benefits, inputs and outputs.
			Figure 6	The outer box was incorrectly labeled and has been updated to read "Shared Responsibility Model."
			Figure 7	Added qualification that the tests listed are notional and are an incomplete list of the types of tests. The complete set of tests to assure the artifact meets mission objectives should be collaboratively defined with DOT&E.
			5. K8s Reference Design Tools and Activities	Updated the section title "Additional Tools and Activities" to more concretely indicate that the set of Tools and Activities that follow in this section are specific to the K8s Reference Design.
			5. K8s Reference Design Tools and Activities	Corrected the reference "part of" to properly read "along with" when referring to two separate documents, the DevSecOps Tools and Activities Guidebook and the DevSecOps Fundamentals.

			Table 7	Removed reference to Security Content Automation Protocol (SCAP) and replaced with the requirement for a structured machine-readable format.
			5.1 Continuous Monitoring in K8s	Explicitly named the DoD Cybersecurity Service Provider (CSSP) as handling a cyber-response.
	DevSecOps Figures (pptx)	1.0	*Initial Release (for re-use of figure clip art)*	
	DRAFT Reference Design: AWS Managed Services	0.2	Initial Draft Release. *Highly immature, pending 3PAO assessment of key managed service(s)*	
	DRAFT Reference Design: Multi-Cluster Kubernetes	0.8	Initial Draft Release *Lessons Learned being Captured from Executing Pilots*	
2.0	Initial Document Set Release			