Software Assurance through DevSecOps

Mr. Bradley Lanford
SAIC Contractor Support
Science and Technology Program Protection
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Software Assurance in DevSecOps

- **The DoD has rapidly transitioned to DevSecOps (DSO) in an effort to deliver software at the speed of relevance. Software modernization efforts include:**
  - Standup of approximately 30 organizations providing infrastructure and platform services to programs
  - Updates to Adaptive Acquisition Framework (AAF) policy and supporting guidance
  - Issued DoD Instruction 5000.87 Operation of the Software Acquisition Pathway supporting DoD adoption of DSO
  - Publication of standards and best practices to support program implementation

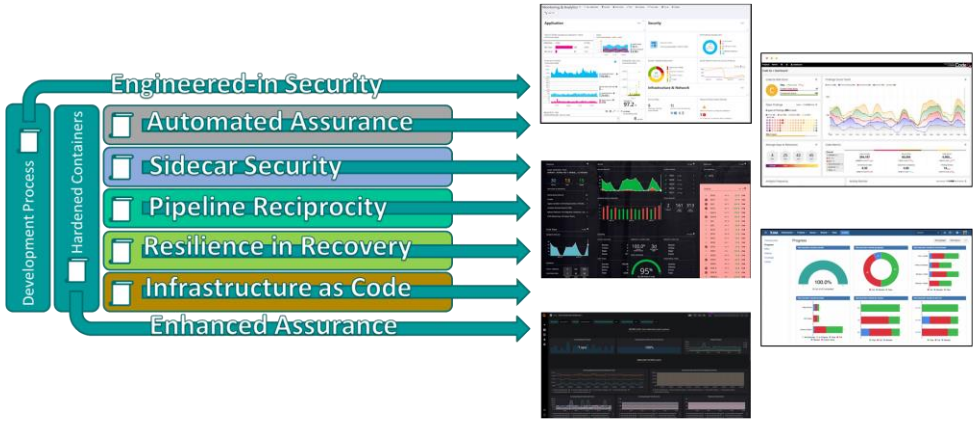
- **The DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," requires programs to employ system security engineering methods and practices, including software assurance (SwA), commensurate with technology, program, system, and mission objectives**
  - OUSD(R&E) STPP is currently updating the Program Protection Planning Outline and Guidance (PPP O&G) to reflect changes to the 5000.83 and support software modernization objectives
  - The automation of manual assurance processes and standardization of risks processes continue to challenge the effectiveness of SwA implementation

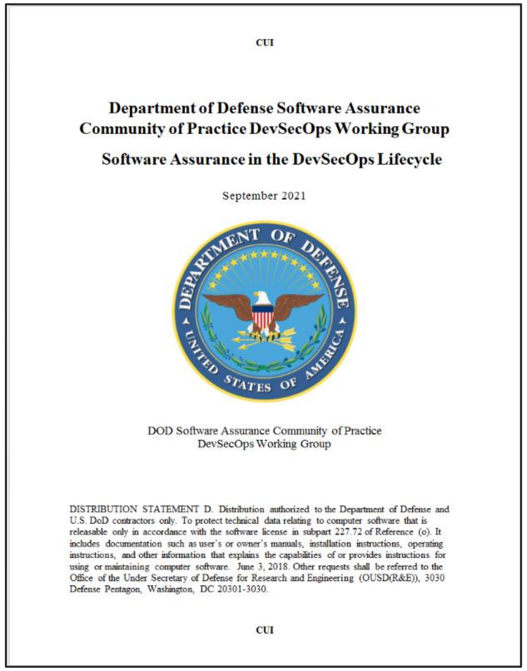
- **As DevSecOps capabilities mature, the Department and industry partners must ensure the implementation of DevSecOps supports both the broad application of SwA practices and can be tailored to protect critical software**

SwA in DevSecOps

Completion of SwA in DevSecOps whitepaper with DoD/NNSA Software Assurance Community of Practice

Alignment of software assurance practices with the DevSecOps lifecycle and generation of artifacts to support decisions





CUI

Department of Defense Software Assurance
Community of Practice DevSecOps Working Group

Software Assurance in the DevSecOps Lifecycle

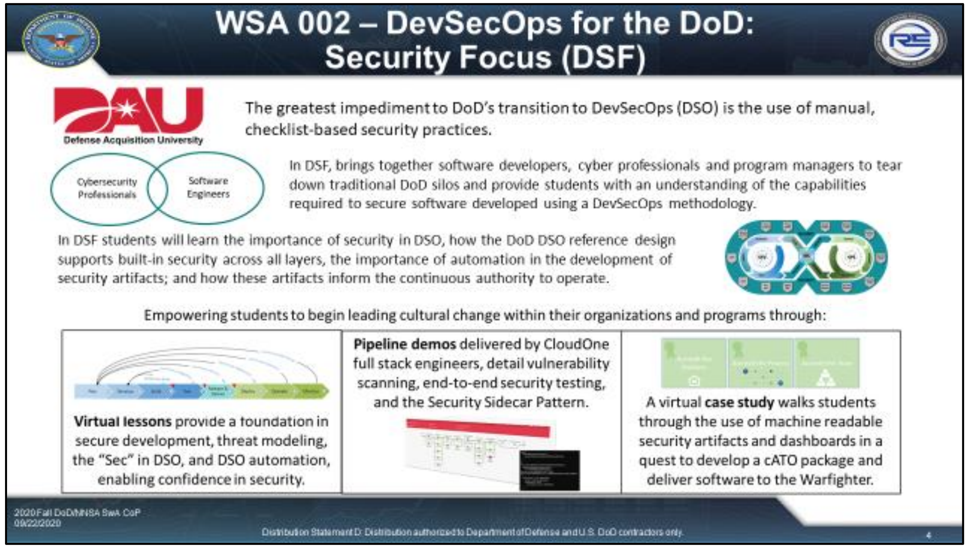
September 2021

DOD Software Assurance Community of Practice
DevSecOps Working Group

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only. To protect technical data relating to computer software that is releasable only in accordance with the software license in subpart 227.72 of Reference (o). It includes documentation such as user's or owner's manuals, installation instructions, operating instructions, and other information that explains the capabilities of or provides instructions for using or maintaining computer software. June 3, 2018. Other requests shall be referred to the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), 3030 Defense Pentagon, Washington, DC 20301-3030.

CUI

Development of DAU WSA 002 – DevSecOps for the DoD: Security Focus (DSF)



WSA 002 – DevSecOps for the DoD: Security Focus (DSF)

Defense Acquisition University

The greatest impediment to DoD's transition to DevSecOps (DSO) is the use of manual, checklist-based security practices.

Cybersecurity Professionals
Software Engineers

In DSF, brings together software developers, cyber professionals and program managers to tear down traditional DoD silos and provide students with an understanding of the capabilities required to secure software developed using a DevSecOps methodology.

In DSF students will learn the importance of security in DSO, how the DoD DSO reference design supports built-in security across all layers, the importance of automation in the development of security artifacts; and how these artifacts inform the continuous authority to operate.

Empowering students to begin leading cultural change within their organizations and programs through:

Virtual lessons provide a foundation in secure development, threat modeling, the "Sec" in DSO, and DSO automation, enabling confidence in security.

Pipeline demos delivered by CloudOne full stack engineers, detail vulnerability scanning, end-to-end security testing, and the Security Sidecar Pattern.

A virtual **case study** walks students through the use of machine readable security artifacts and dashboards in a quest to develop a cATO package and deliver software to the Warfighter.

2020 Fall DoD/NNSA SwA CoP
09/22/2020

Distribution Statement D: Distribution authorized to Department of Defense and U.S. DoD contractors only.

4

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Software Assurance Gaps 2020

Hardened Container SRG

Existing DevSecOps service provider capabilities use automated scanning (OpenSCAP, Anchor, Twistlock) focusing on cybersecurity STIG and known vulnerability assessments. Opportunity for enhanced assurance capabilities.

Assurance Baseline and critical function assessments

Pipeline adoption continues to utilize a small subset of assurance tools and lacks consideration of raised assurance level for critical components.

Software Threat Modeling

Iterative threat modeling established through development process and cadence. Limited automation and MBSE maturity to support CI/CD.

Analysis Data Strategy

Correlation of analysis findings and data strategy for pipeline data artifacts impact programs ability to effectively use assurance tools.

Risk Categorization/Tolerance

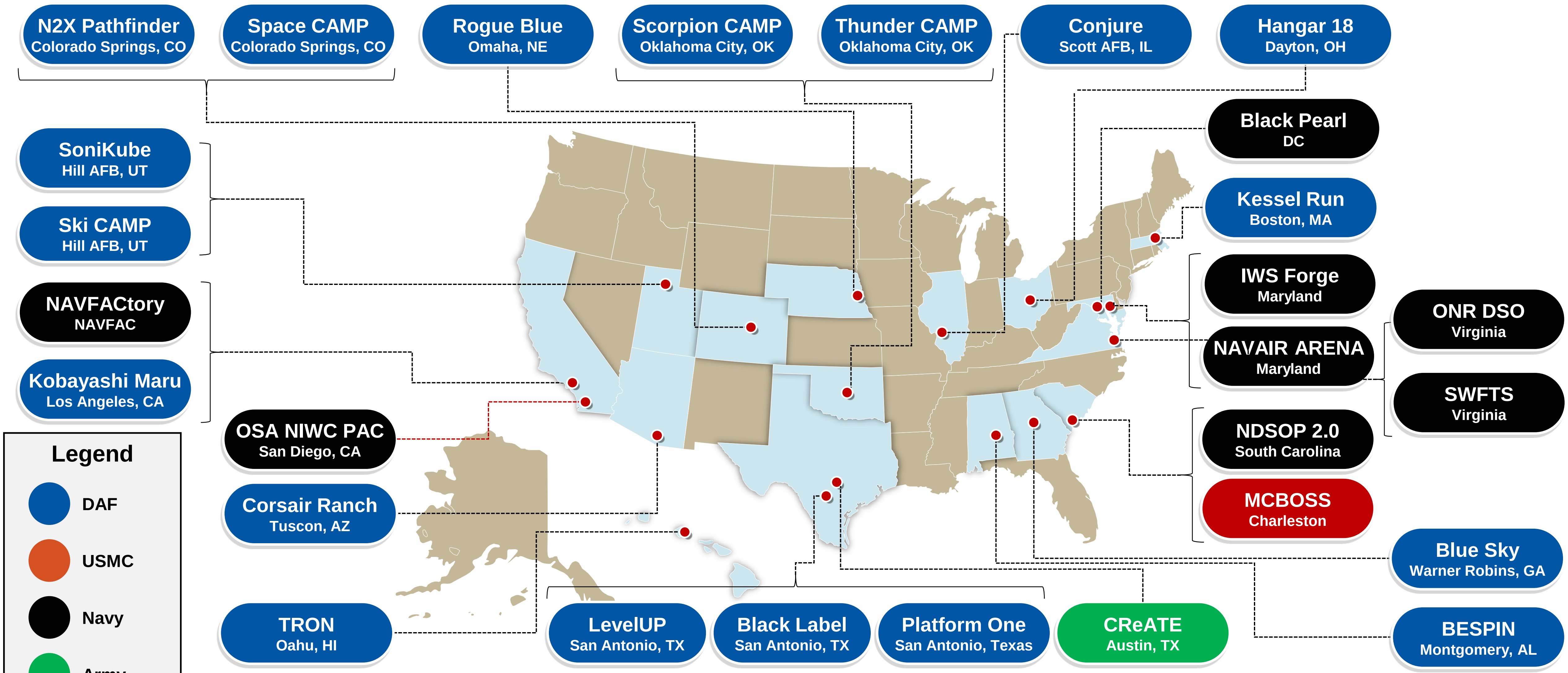
Standard process for risk categorization and process to establish risk tolerance based on assurance level does not exist. Does not support

Open Source Assurance

Limited understanding of Software Supply Chain for Open Source and COTS continues to be a source of risk.

The automation of manual assurance processes and standardization of risks processes impede SwA adoption for DSO

Scope of DevSecOps in the DoD



N2X Pathfinder
Colorado Springs, CO

Space CAMP
Colorado Springs, CO

Rogue Blue
Omaha, NE

Scorpion CAMP
Oklahoma City, OK

Thunder CAMP
Oklahoma City, OK

Conjure
Scott AFB, IL

Hangar 18
Dayton, OH

SoniKube
Hill AFB, UT

Ski CAMP
Hill AFB, UT

NAVFACtory
NAVFAC

Kobayashi Maru
Los Angeles, CA

OSA NIWC PAC
San Diego, CA

Corsair Ranch
Tuscon, AZ

TRON
Oahu, HI

LevelUP
San Antonio, TX

Black Label
San Antonio, TX

Platform One
San Antonio, Texas

CReATE
Austin, TX

Black Pearl
DC

Kessel Run
Boston, MA

IWS Forge
Maryland

NAVAIR ARENA
Maryland

ONR DSO
Virginia

SWFTS
Virginia

NDSOP 2.0
South Carolina

MCBOSS
Charleston

Blue Sky
Warner Robins, GA

BESPIN
Montgomery, AL

Legend

🔵 DAF

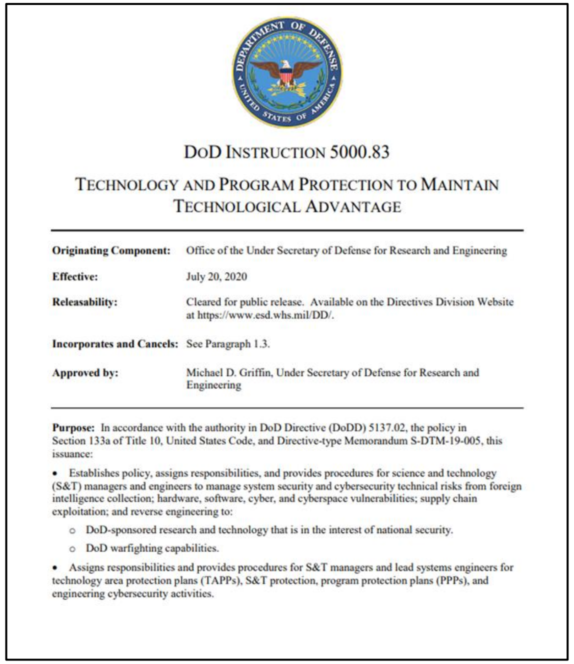
🟠 USMC

⚫ Navy

🟢 Army

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

DoDI 5000.83 Technology and Program Protection



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

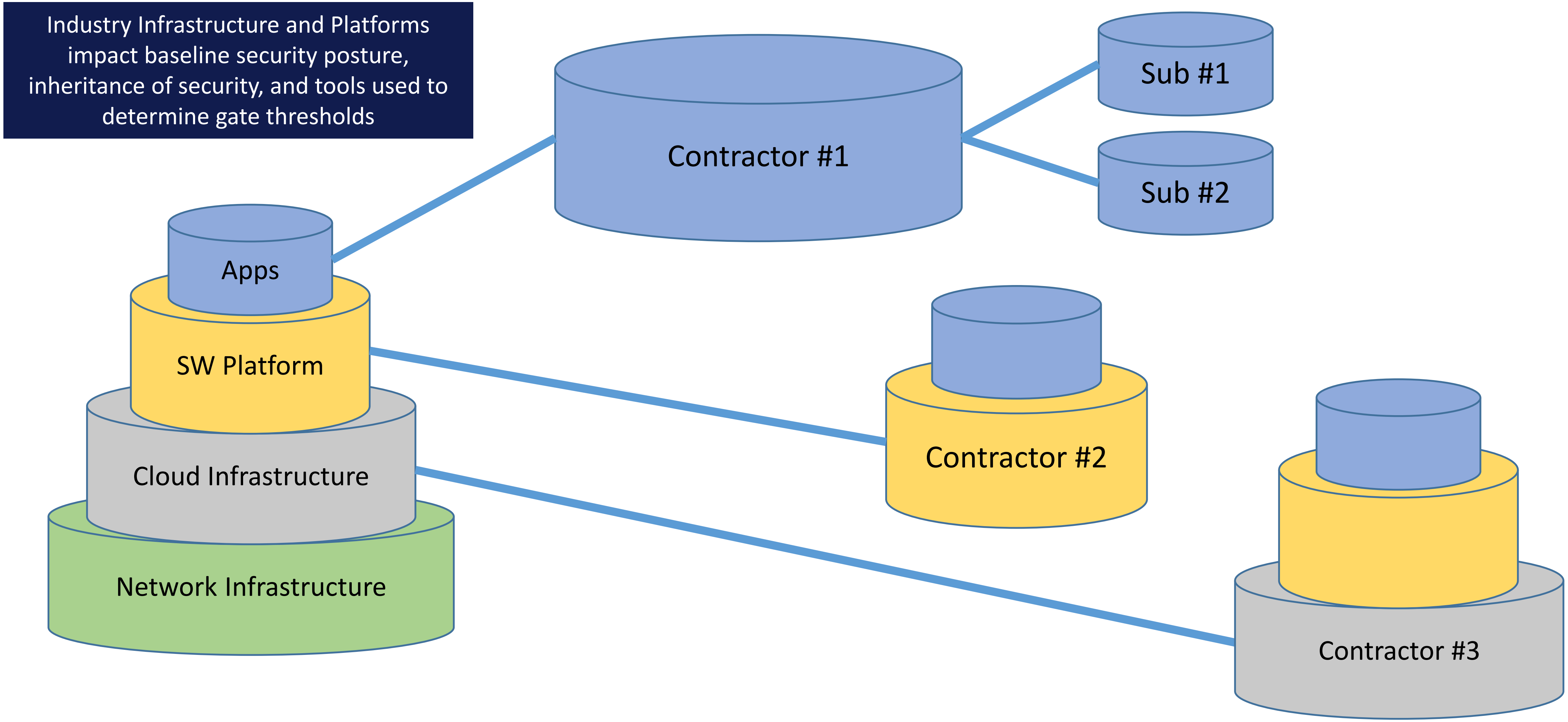
DoDI 5000.83, “Technology and Program Protection to Maintain Technological Advantage”

Programs will employ **system security engineering methods and practices**, including cybersecurity, cyber resilience, and cyber survivability in design, test, manufacture, and sustainment. Such methods and practices will ensure that systems function as intended, mitigating risks associated with **known and exploitable vulnerabilities** to provide a **level of assurance** commensurate with technology, program, system, and mission objectives.

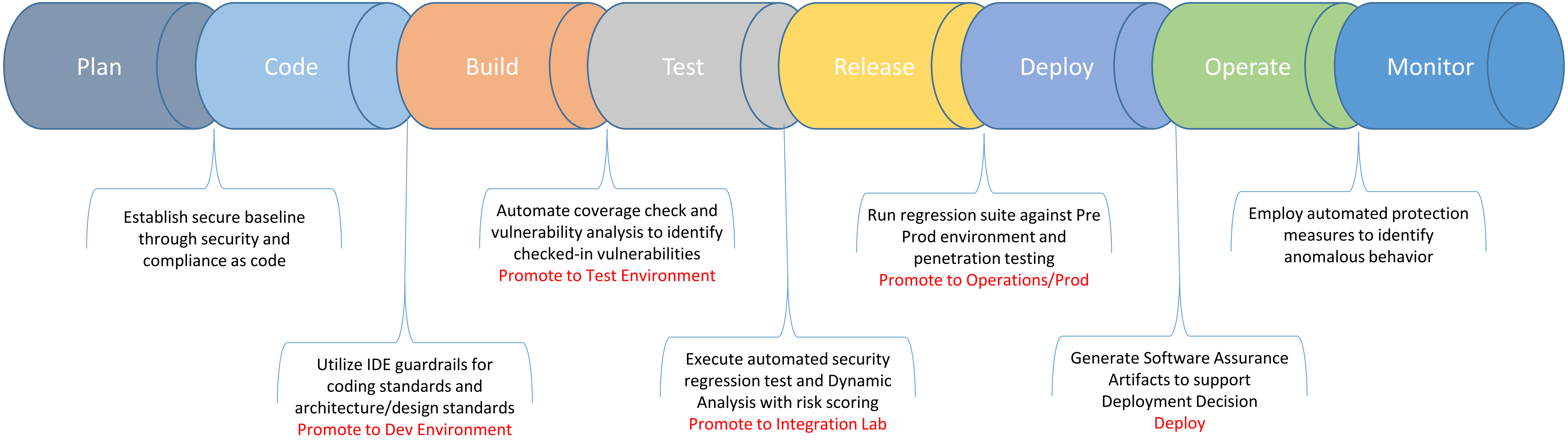
Selection of DevSecOps tools supporting program protection must be informed by technology, program, system, and mission objectives

Relationship to Industry Partners (Infrastructure and Platform)

Industry Infrastructure and Platforms impact baseline security posture, inheritance of security, and tools used to determine gate thresholds



SwA in the CI/CD pipeline



Plan

Code

Build

Test

Release

Deploy

Operate

Monitor

Establish secure baseline through security and compliance as code

Utilize IDE guardrails for coding standards and architecture/design standards
Promote to Dev Environment

Automate coverage check and vulnerability analysis to identify checked-in vulnerabilities
Promote to Test Environment

Execute automated security regression test and Dynamic Analysis with risk scoring
Promote to Integration Lab

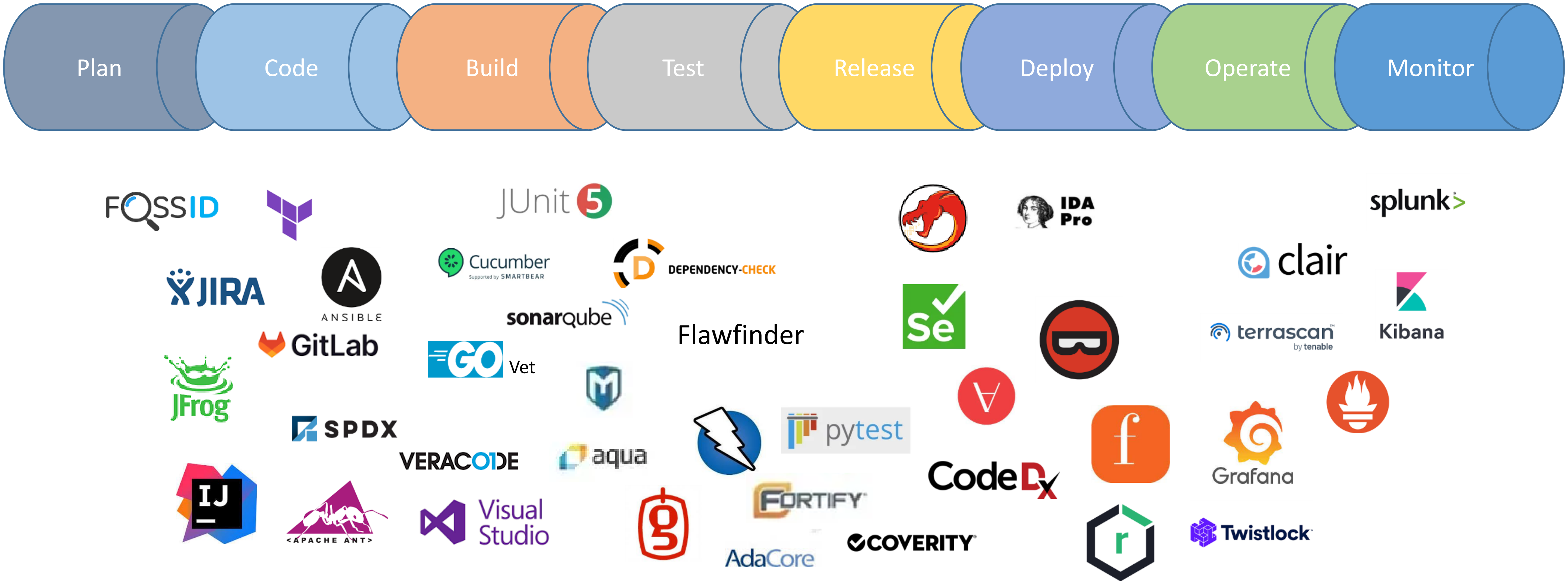
Run regression suite against Pre Prod environment and penetration testing
Promote to Operations/Prod

Generate Software Assurance Artifacts to support Deployment Decision
Deploy

Employ automated protection measures to identify anomalous behavior

CI/CD automation establishes gates where assurance thresholds can be evaluated prior to promotion of software builds. Vulnerabilities can delay deployment, or risk can be accepted and tracked.

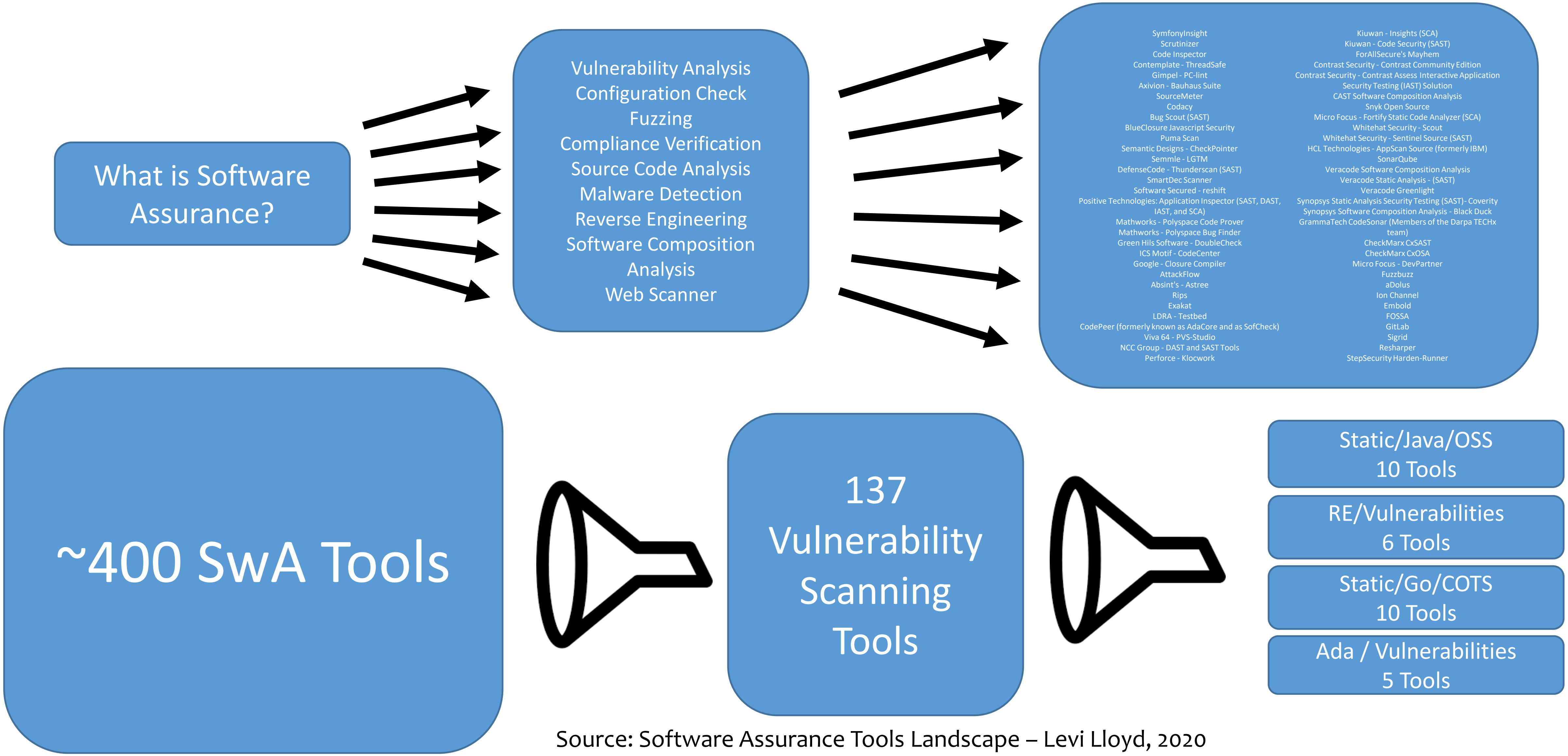
SwA Tool Mapping to DSO



Security tools and capabilities integrated into common DevSecOps tools provide assurance across the DSO lifecycle

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

SwA Tool Story



What is Software Assurance?

Vulnerability Analysis
Configuration Check
Fuzzing
Compliance Verification
Source Code Analysis
Malware Detection
Reverse Engineering
Software Composition Analysis
Web Scanner

SymfonyInsight
Scrutinizer
Code Inspector
Contemplate - ThreadSafe
Gimpel - PC-lint
Axivion - Bauhaus Suite
SourceMeter
Codacy
Bug Scout (SAST)
BlueClosure Javascript Security
Puma Scan
Semantic Designs - CheckPointer
Semmle - LGTM
DefenseCode - Thunderscan (SAST)
SmartDec Scanner
Software Secured - reshift
Positive Technologies: Application Inspector (SAST, DAST, IAST, and SCA)
Mathworks - Polyspace Code Prover
Mathworks - Polyspace Bug Finder
Green Hils Software - DoubleCheck
ICS Motif - CodeCenter
Google - Closure Compiler
AttackFlow
Absint's - Astree
Rips
Exakat
LDRA - Testbed
CodePeer (formerly known as AdaCore and as SofCheck)
Viva 64 - PVS-Studio
NCC Group - DAST and SAST Tools
Perforce - Klocwork

Kiuwan - Insights (SCA)
Kiuwan - Code Security (SAST)
ForAllSecure's Mayhem
Contrast Security - Contrast Community Edition
Contrast Security - Contrast Assess Interactive Application Security Testing (IAST) Solution
CAST Software Composition Analysis
Snyk Open Source
Micro Focus - Fortify Static Code Analyzer (SCA)
Whitehat Security - Scout
Whitehat Security - Sentinel Source (SAST)
HCL Technologies - AppScan Source (formerly IBM)
SonarQube
Veracode Software Composition Analysis
Veracode Static Analysis - (SAST)
Veracode Greenlight
Synopsys Static Analysis Security Testing (SAST)- Coverity
Synopsys Software Composition Analysis - Black Duck
GrammaTech CodeSonar (Members of the Darpa TECHx team)
CheckMarx CxSAST
CheckMarx CxOSA
Micro Focus - DevPartner
Fuzzbuzz
aDolus
Ion Channel
Embold
FOSSA
GitLab
Sigrid
Resharper
StepSecurity Harden-Runner

~400 SwA Tools

137 Vulnerability Scanning Tools

Static/Java/OSS
10 Tools

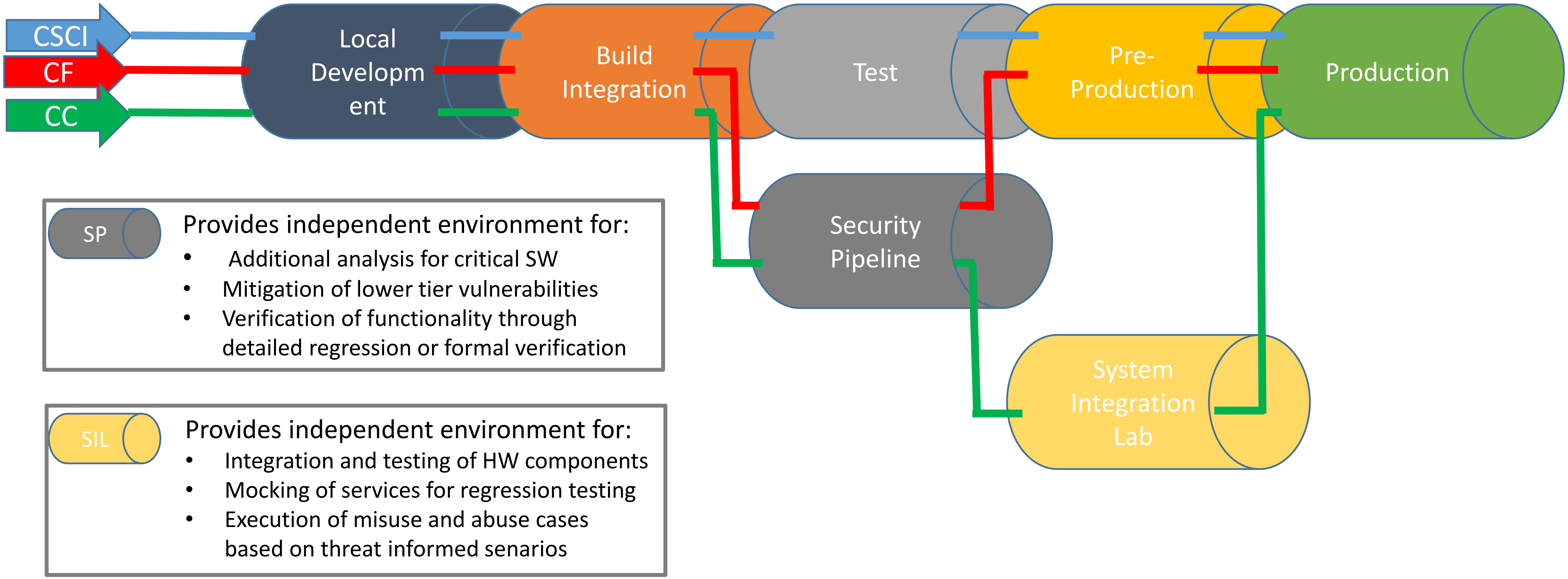
RE/Vulnerabilities
6 Tools

Static/Go/COTS
10 Tools

Ada / Vulnerabilities
5 Tools

Source: Software Assurance Tools Landscape – Levi Lloyd, 2020

Level of Assurance



Provides independent environment for:

- Additional analysis for critical SW
- Mitigation of lower tier vulnerabilities
- Verification of functionality through detailed regression or formal verification

Provides independent environment for:

- Integration and testing of HW components
- Mocking of services for regression testing
- Execution of misuse and abuse cases based on threat informed senarios

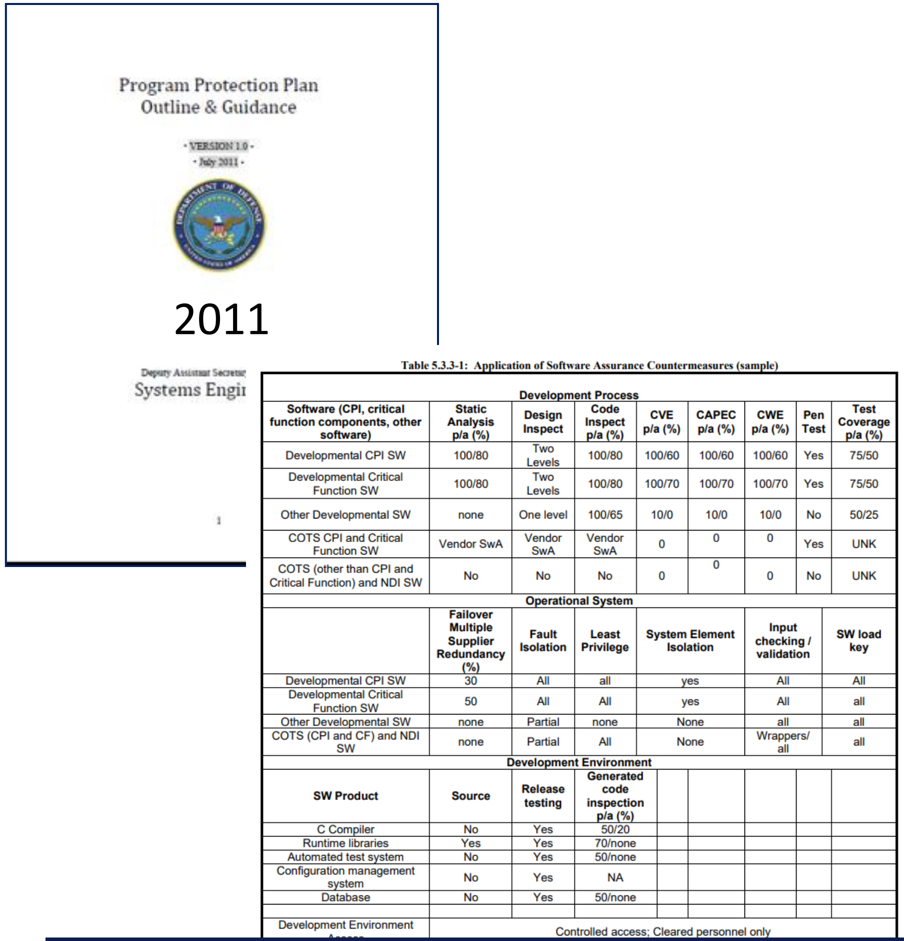
Increased levels of assurance in DSO requires programs to establish more rigorous testing and pre-production environments, ensuring assurance is commensurate with technology, program, system, and mission objectives

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

PPP O&G SwA Table Mapping to DSO

PPP O&G 2011 SwA Section



Program Protection Plan
Outline & Guidance

- VERSION 1.0 -
- July 2011 -

2011

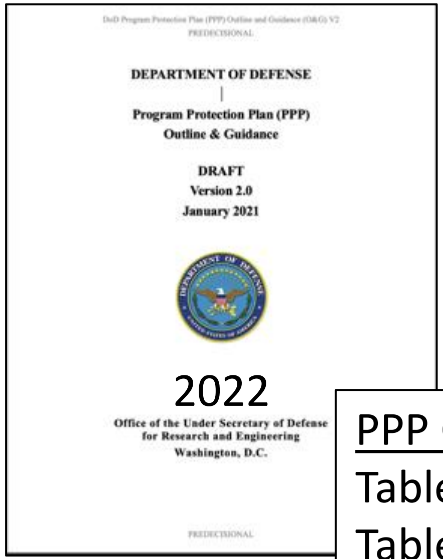
Deputy Assistant Secretar
Systems Engi

1

Table 5.3.3-1: Application of Software Assurance Countermeasures (sample)

Development Process									
Software (CPI, critical function components, other software)	Static Analysis p/a (%)	Design Inspect	Code Inspect p/a (%)	CVE p/a (%)	CAPEC p/a (%)	CWE p/a (%)	Pen Test	Test Coverage p/a (%)
Developmental CPI SW	100/80	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50
Developmental Critical Function SW	100/80	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK
Operational System									
	Failover Multiple Supplier Redundancy (%)	Fault Isolation	Least Privilege	System Element Isolation		Input checking / validation		SW load key
Developmental CPI SW	30	All	all	yes		All		All
Developmental Critical Function SW	50	All	All	yes		All		all
Other Developmental SW	none	Partial	none	None		all		all
COTS (CPI and CF) and NDI SW	none	Partial	All	None		Wrappers/ all		all
Development Environment									
SW Product	Source	Release testing	Generated code inspection p/a (%)					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment Access	Controlled access; Cleared personnel only							

PPP O&G 2022 SwA Section



DoD Program Protection Plan (PPP) Outline and Guidance (O&G) V2
PREDECISIONAL

DEPARTMENT OF DEFENSE

Program Protection Plan (PPP)
Outline & Guidance

DRAFT
Version 2.0
January 2021

2022

Office of the Under Secretary of Defense
for Research and Engineering
Washington, D.C.

PREDECISIONAL

PPP O&G SwA Sections

Table 2-12 SW Infrastructure
Table 2-13 Software Scope
Table 2-14 Software Process
Table 2-15 SW Methods Practices and Tools
Table 2-16 SW Environments Summary
Table 2-17 SW Weaknesses and vulnerabilities
Table 2-18 SW Protections
Table 2-21 SW Procurement

Updated PPP O&G tables support tracking of assurance methods, practices and protections for infrastructure, environments, and assurance tools

Transparency, Data, and Confidence

Plan
- SwA Requirements
- Secure Design Considerations
- Threat Model

Code
- Coding Standards
- IDE configurations
- Unit Test Cases

Build
- Static Analysis Findings
- Software composition
- Security & Configuration as Code

Test
- Static Dynamic Analysis Results
- Prioritized Vulnerabilities

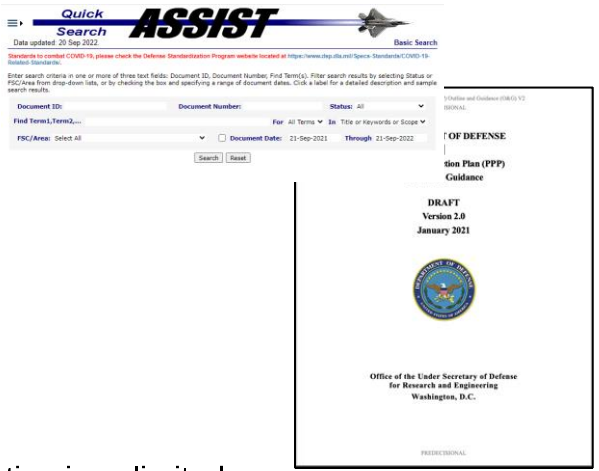
Release
- Pre-production regression results
- Penetration Testing Findings

Deploy
- Software Bill of Materials
- Residual Risks
- Deviation from gate thresholds

Operate
- Verification of user behavior
- SW updates

Monitor
- Anomalous Behavior Response
- Alerts

Data Item Descriptions should include artifacts that provide decision makers with confidence that software is adequately protected and that protection measures have been employed to mitigate risks



Quick Search ASSIST

Data updated: 20 Sep 2022

Basic Search

Standards to combat COVID-19, please check the Defense Standardization Program website located at https://www.dsp.dla.mil/Specs-Standards/COVID-19-Related-Standards/.

Enter search criteria in one or more of three text fields: Document ID, Document Number, Find Term(s). Filter search results by selecting Status or FSC/Area from drop-down lists, or by checking the box and specifying a range of document dates. Click a label for a detailed description and sample search results.

Document ID:
Document Number:
Status: All
Find Term1,Term2,...
For All Terms In Title or Keywords or Scope
FSC/Area: Select All
□ Document Date: 21-Sep-2021 Through 21-Sep-2022

Search Reset

) Outline and Guidance (O&G) V2
SIONAL

T OF DEFENSE

tion Plan (PPP)
Guidance

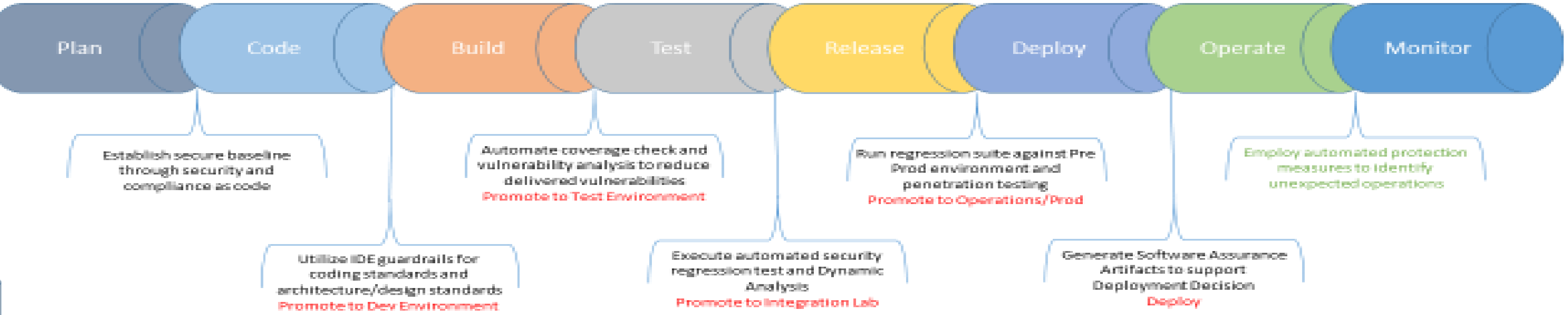
DRAFT
Version 2.0
January 2021

Office of the Under Secretary of Defense
for Research and Engineering
Washington, D.C.

PREDECISIONAL

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

PPP O&G SwA Table Mapping to DSO



Establish secure baseline through security and compliance as code

Utilize IDE guardrails for coding standards and architecture/design standards
Promote to Dev Environment

Automate coverage check and vulnerability analysis to reduce delivered vulnerabilities
Promote to Test Environment

Execute automated security regression test and Dynamic Analysis
Promote to Integration Lab

Run regression suite against Pre Prod environment and penetration testing
Promote to Operations/Prod

Generate Software Assurance Artifacts to support Deployment Decision
Deploy

Employ automated protection measures to identify unexpected operations

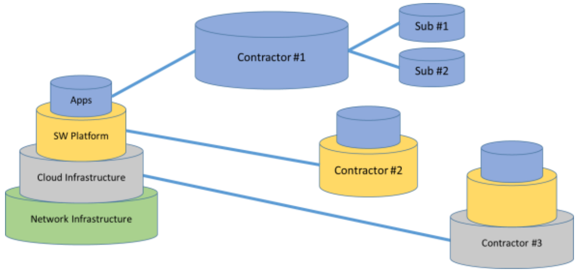


Table 2-12
Software Infrastructure

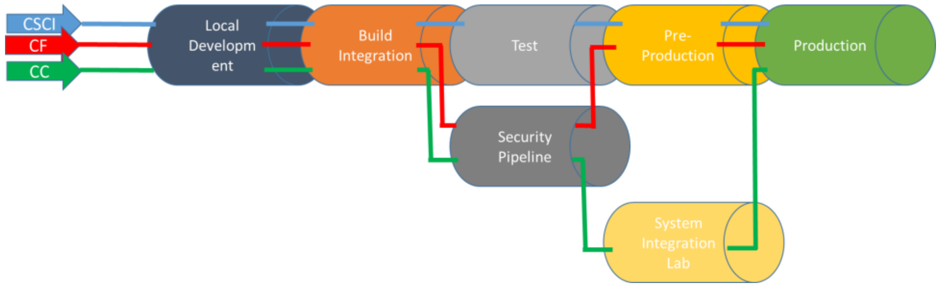
Table 2-13
Software Scope

Table 2-14
Software Process

Table 2-15
SW Methods
Practices and Tools

Table 2-17
SW Weaknesses and
vulnerabilities

Table 2-16
SW Environments Summary



<u>Table 2-18 SW Protections</u>
Operating Systems
Language Selection
Standards
Security Sidecar

Table 2-21
<u>Software Procurement</u>
Vendor SwA Process
SW Bill of Materials
Protection Measures

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Summary

- **DoD Adoption of DevSecOps and the availability of automated tools are enhancing program's ability to implement software assurance**

- **Acquisition processes and the contractual relationship to industry partners create boundaries not present in commercial software development. These boundaries also impact program confidence in the systems assurance including:**
  - Security and Configuration across PaaS and IaaS solutions
  - Tool customization to support technology, program, system, and mission objectives
  - Design of integration and test environments to mirror operations
  - Delivery of assurance artifacts to support risk decisions

- **OUSD(R&E) STPP (Systems Security directorate) updates to the PPP O&G and supporting DIDs will enable the planning and execution of software assurance in a DevSecOps ecosystem**

- **Industry support, review, and feedback on Software Assurance DID is welcomed and appreciated**

Questions?

Bradley Lanford

SAIC Contractor Support

Office of the Under Secretary of Defense
for Research and Engineering

bradley.p.lanford.ctr@mail.mil

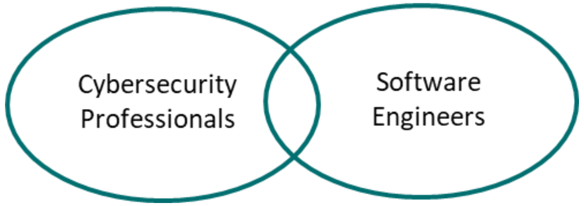
Backup

Backup Slides

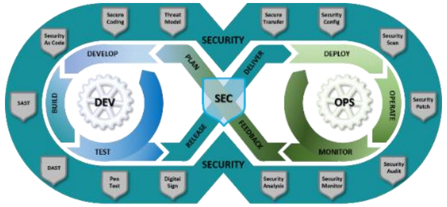
WSA 002 – DevSecOps for the DoD: Security Focus (DSF)

Defense Acquisition University

The greatest impediment to DoD's transition to DevSecOps (DSO) is the use of manual, checklist-based security practices.

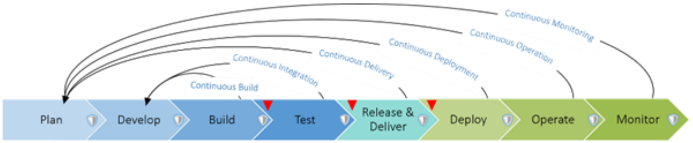


In DSF, brings together software developers, cyber professionals and program managers to tear down traditional DoD silos and provide students with an understanding of the capabilities required to secure software developed using a DevSecOps methodology.



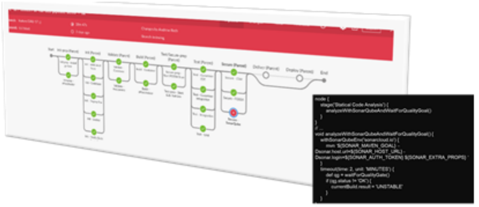
In DSF students will learn the importance of security in DSO, how the DoD DSO reference design supports built-in security across all layers, the importance of automation in the development of security artifacts; and how these artifacts inform the continuous authority to operate.

Empowering students to begin leading cultural change within their organizations and programs through:



Virtual lessons provide a foundation in secure development, threat modeling, the "Sec" in DSO, and DSO automation, enabling confidence in security.

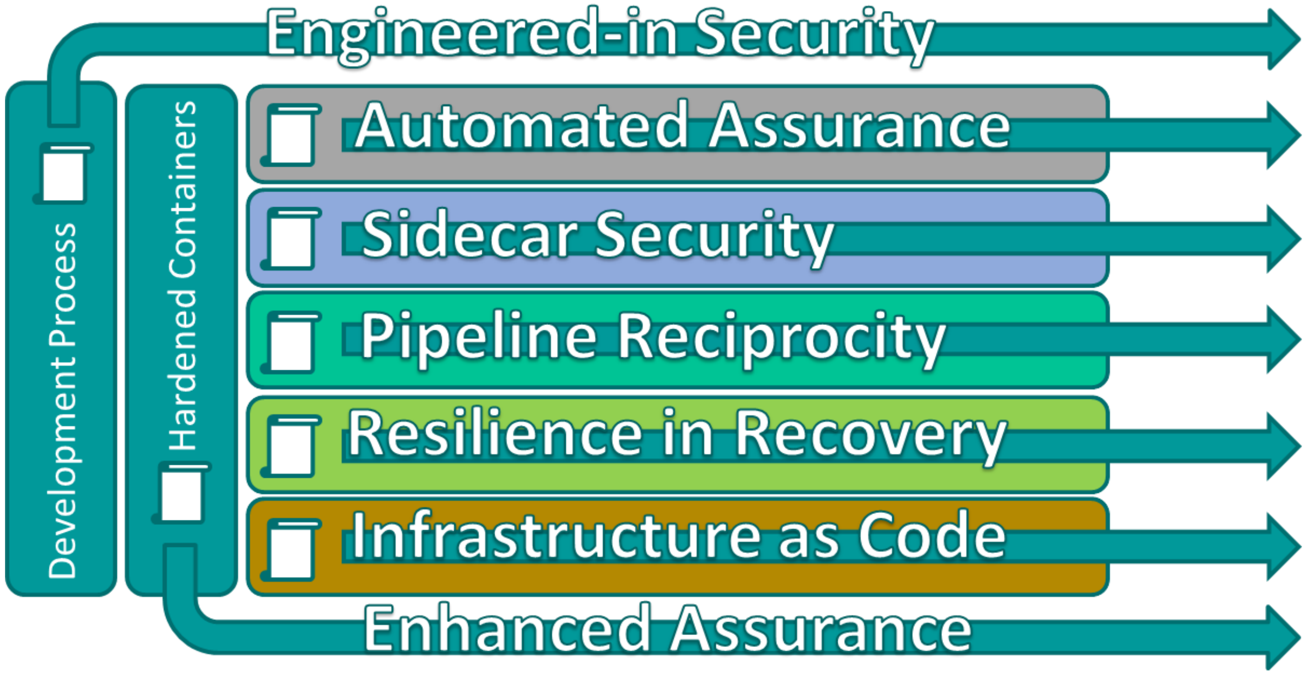
Pipeline demos delivered by CloudOne full stack engineers, detail vulnerability scanning, end-to-end security testing, and the Security Sidecar Pattern.



A virtual **case study** walks students through the use of machine readable security artifacts and dashboards in a quest to develop a cATO package and deliver software to the Warfighter.

Distribution Statement A: Approved for public release. DOPSR case #23-S-0063 applies. Distribution is unlimited.

Continuous Verification of Assurance



Development Process

Hardened Containers

Engineered-in Security

Automated Assurance

Sidecar Security

Pipeline Reciprocity

Resilience in Recovery

Infrastructure as Code

Enhanced Assurance