USD(R&E)

DoD Software Modernization and the Program Protection Plan

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
October 17-19, 2023

Software Assurance in DevSecOps

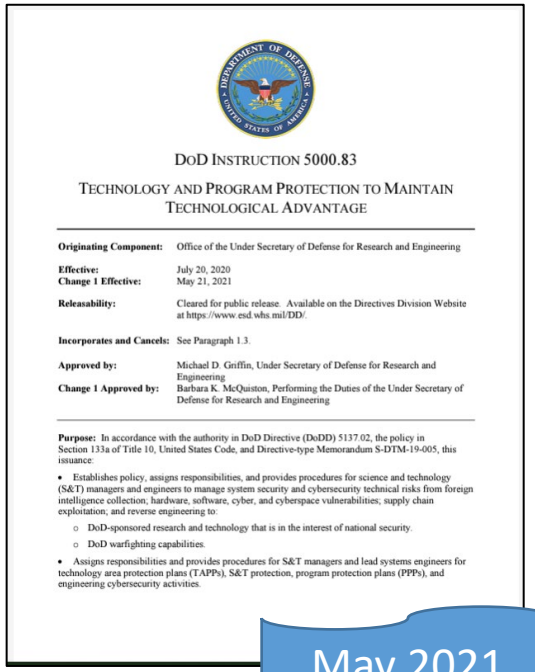
- **DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," requires programs to employ system security engineering methods and practices, including software assurance (SwA), commensurate with technology, program, system, and mission objectives**

- **The DoD Software Modernization Strategy implementation plan identifies 10 tasks designed to increase technological capabilities across the Department and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena. The tasks support 3 Software Modernization Goals:**
  - Accelerate the DoD Enterprise Cloud Environment
  - Establish Department-wide Software Factory Ecosystem
  - Transform Processes to Enable Resilience and Speed

OUSD(R&E) STPP is updating the Program Protection Planning Outline and Guidance (PPP O&G) to reflect changes to the 5000.83 and support software modernization objectives including:

- Inheritance of software protections through infrastructures, platforms, and tool pipelines
- Assured integration of COTS and Open-Source software to deliver capability at the speed of relevance
- Advancement of the software workforce to deliver secure software capabilities

DoD Software Modernization and Software Assurance Timeline



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
Change 1 Effective: May 21, 2021

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

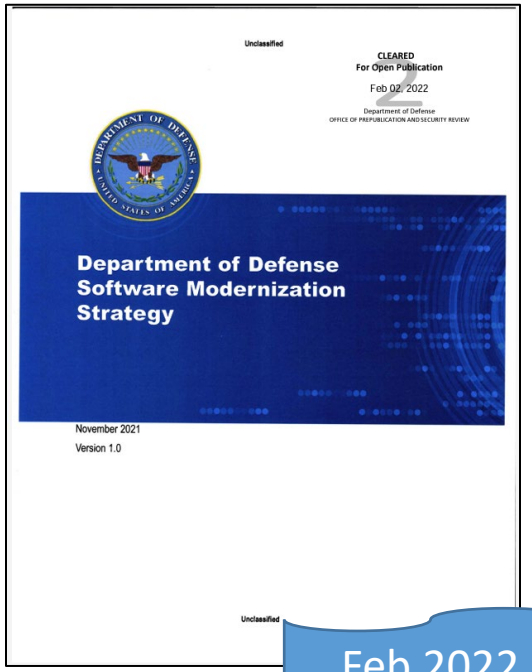
Incorporates and Cancels: See Paragraph 1.3.

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering
Change 1 Approved by: Barbara K. McQuiston, Performing the Duties of the 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.

May 2021



Unclassified

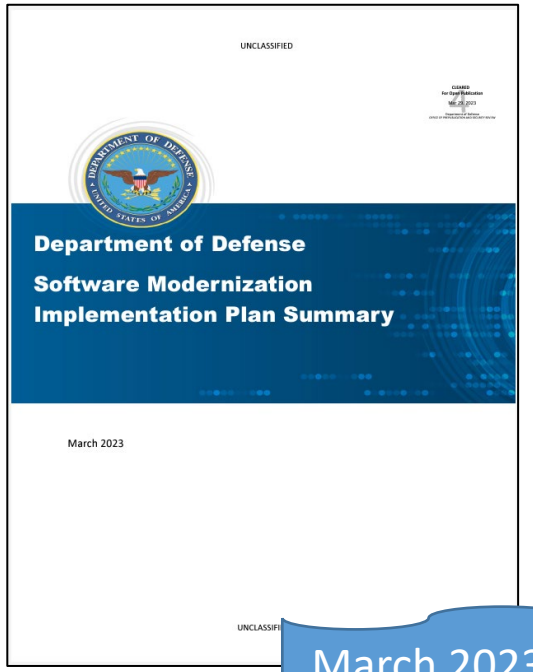
CLEARED
For Open Publication
Feb 02, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense
Software Modernization
Strategy

November 2021
Version 1.0

Unclassified

Feb 2022



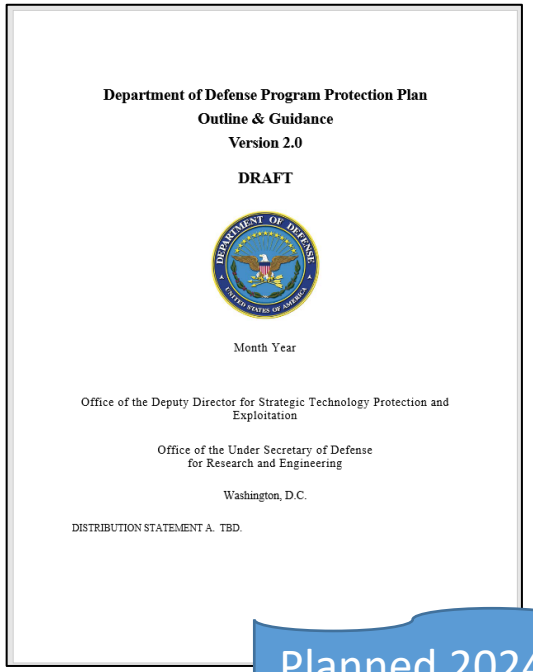
UNCLASSIFIED

Department of Defense
Software Modernization
Implementation Plan Summary

March 2023

UNCLASSIFI

March 2023



Department of Defense Program Protection Plan
Outline & Guidance
Version 2.0

DRAFT

Month Year

Office of the Deputy Director for Strategic Technology Protection and Exploitation

Office of the Under Secretary of Defense
for Research and Engineering

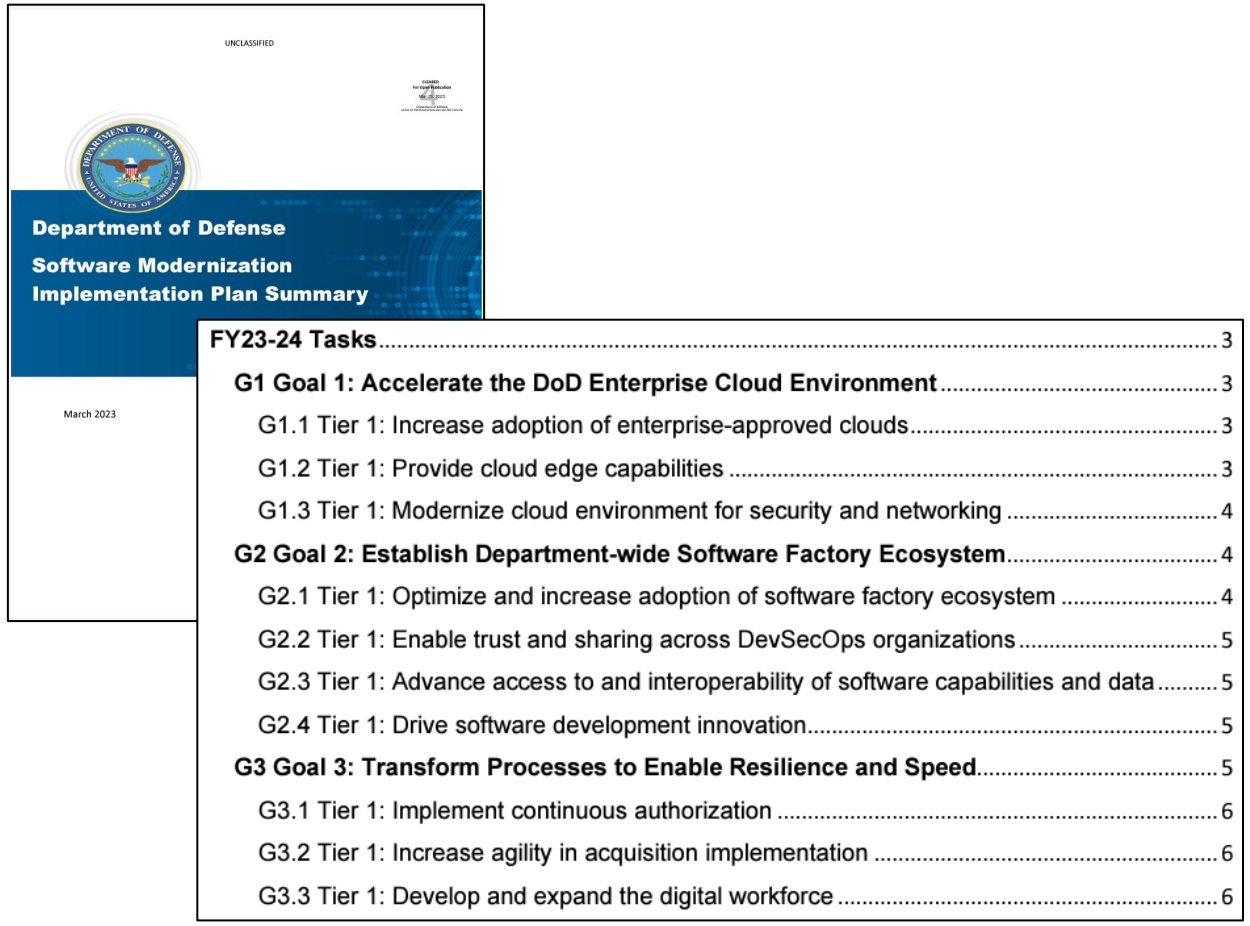
Washington, D.C.

DISTRIBUTION STATEMENT A. TBD.

Planned 2024

The software modernization strategy identifies capabilities that are critical to the departments ability to deliver software solutions to the warfighter. Program protection practices must also modernize to ensure the implementation of these capabilities positively impacts our ability to protect them

Software Assurance in Software Modernization



UNCLASSIFIED

Department of Defense
Software Modernization
Implementation Plan Summary

March 2023

- **Inheritance of assurance through adoption of infrastructure and platforms**
- **Integration of assurance tools into DoD Software factory pipelines**
- **Analysis and sharing of assured software (COTS, GOTS, and Open Source)**
- **Establishing SwA thresholds for promotion of software**
- **Promote the use of modern software frameworks, technologies and languages**
- **Advance the SwA workforce through DAU SwA Credentials**

Proposed PPP O&G SwA Table Mapping to DevSecOps (NDIA SE 2022)

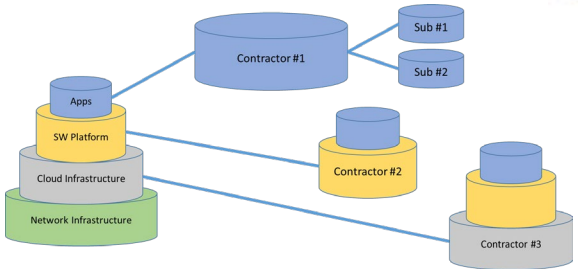


Table 2-12
Software Infrastructure

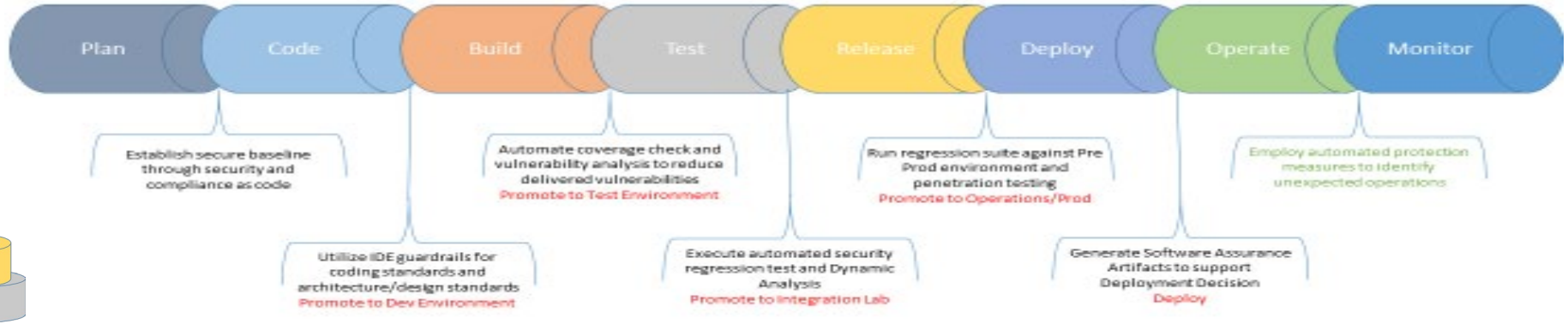


Table 2-13
Software Scope

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

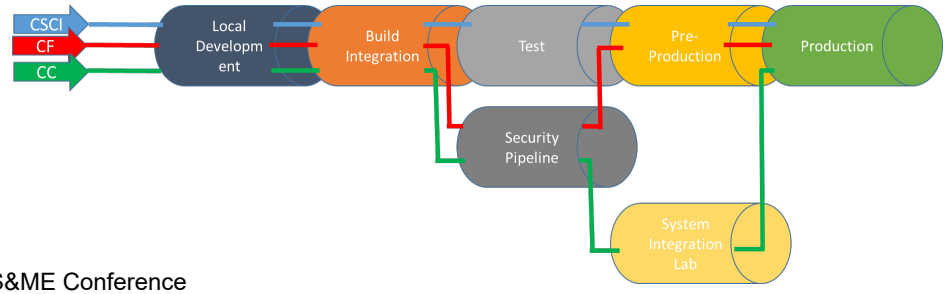


Table 2-18
SW Protections

Operating Systems
Language Selection
Standards
Security Sidecar

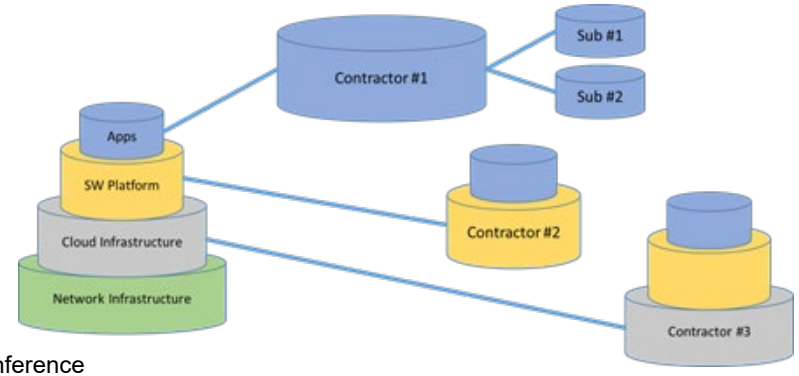
Table 2-21
Software Procurement

Vendor SwA Process
SW Bill of Materials
Protection Measures

Inheritance of Assurance Through Adoption of Infrastructure and Platforms

PPP Outline & Guidance Approach:

- Allows Program Management Office to identify government owned and operated, government owned and contractor operated, and contractor owned and operated network, cloud, or cloud service
- Enables inheritance of cloud provider or contractor implemented security practices
- Informs selection of additional protections at the platform or application level



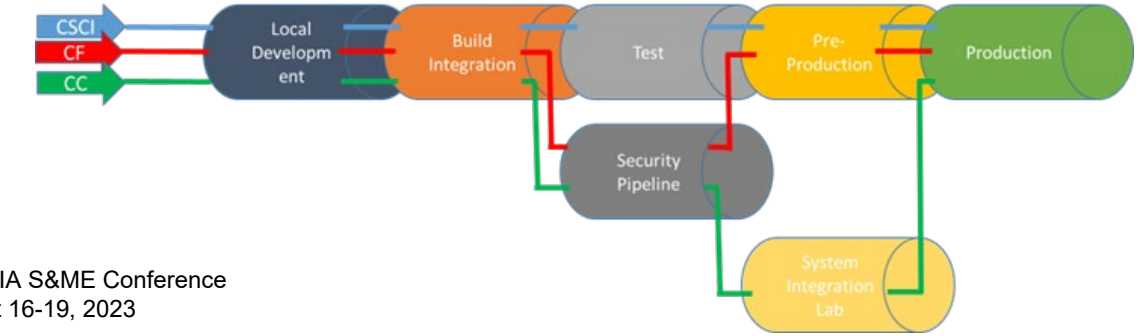
Program Protection Plan Outline and Guidance
Software Infrastructure Protections (Notional Examples)

ID	Infrastructure	Owner and Operator	Purpose or Capability	Classification / Impact Level	Inherited Protection Measures	Applied Protection Measures	Accreditation (type/org/date)	References
INF 1	Contractor A Network	Contractor	Development Environment	U	MS Cloud FedRamp Authorized Infrastructure National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF)	Software Development Plan (SDP), Third Party Penetration Testing,	Contractor A 2022	SDP A
INF 2	Commercial Cloud, Information Impact Level 4	Program Management Office/ Contractor	Integration, Test & Operational Environments	CUI / IL-3 - S / IL-6	Commercial Cloud Security Policy	Penetration testing, Persistent Cyber Operations, Cybersecurity Service Provider (CSSP)	ATO U.S. Navy 2021	Additional proprietary information can be made available upon request
INF 3	Platform One (PaaS)	USAF/ Contractor B	Development Environment	IL-3	Inherited protections identified in DSO Reference Design	Penetration testing, Persistent Cyber Operations, CSSP	ATO USAF 2022	https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
INF 4	Stratus	DISA	Hosting, Storage, Computing Environment	S / IL-6	Vulnerability Management Service Cloud Plus CSSP Services	Penetration testing, Persistent Cyber Operations	ATO U.S. Army 2021	https://www.hacc.mil

Integration of Assurance Tools into DoD Software factory Pipelines

PPP Outline & Guidance Approach:

- Shift in focus from coverage to in breadth of automated assurance tools used across development, test, and production environments.
- Enables Program Management Office to identify tools based on the characteristics and criticality of the software
- Supports continuous integration, stand along security pipelines, and use of specialized environments (SIL, Test Range, etc.)
- Informs protection of software to provide a level of assurance commensurate with technology, program, system and mission objectives.



Software Methods, Practices and Tools (Notional Examples)

Tools and Techniques for PPP Traceability ID	Tools and Techniques Name or Description	Analysis Type	Software Language	Code Format (Binary, Source Code)	Finding Types	Tool Source
TT 1	Analysis Tool #1 (Tool 1)	Static	C++	Binary	Vulnerabilities	Program Office
TT 2	Analysis Tool #2	Static	Java	Source Code	CWEs	Joint Federated Assurance Center (JFAC)
TT 3	Code Review (Technique 2)	Manual	All	Source Code	Failed merge requests	DISA
TT 4	Threat Model	Manual	N/A	N/A	Threat diagram	Open Wor App Se Pr (OV
TT 5	Reverse Engineering	Manual	C++	Binary	Vulnerabilities	N
TT 6	Formal Methods	Manual	N/A	N/A	Verified requirements	DA
TT 7	IDE #1	N/A	C++	Source Code	Coding Standard Compliance	Ver
TT 8	Unit Testing	N/A	C++	N/A	Coverage	Ver
TT 9	Regression Tests	Static/Dynamic	N/A	N/A	Vulnerabilities	Ver
TT 10	Git Repo	Static/Dynamic	N/A	Source	Vulnerabilities	Ver
TT 11	Orchestration	Dynamic	N/A	N/A	N/A	C Sc

Environments Summary (Notional Examples)

Environment Name / ID	Host Infrastructure(Table 9-2)	Environment Owner / Operator	Software ID for PPP Traceability (Table 9-3)	Techniques and Tools for PPP Traceability (Table 9-5)	Supplemental Protection Required	References
Development #1 ENV 1	INF 1	Contractor A	SCO 1	TT 1-5,7-11	SSDF	Propriatary; can be provided with request
Development #2 ENV 2	INF 3	PMO	SCO 2	TT 2, 3, 7	N/A	https://p1.dso.mil/products/party-bus
Integration #1 ENV 3	INF 2	PMO / Contractor A	SCO 1 SCO 2	TT 1, 3, 10-11	Hardened Container SRG	SDP page 3 Development, Security, and Operations (DevSecOps) Tool Chain
Testing #1 ENV 4	INF 2	PMO / Contractor A	SCO 1 SCO 2	TT 2, 5	N/A	Test Plan pg. 4
System Integration Lab ENV 5	N/A	PMO	SCO 1 SCO 2 SCO 3	TT 1	Non-networked environment	Test Plan pg. 6
Production ENV 6	INF 2	PMO	SCO 1, SCO 2,SCO3	TT 1	Cloud security policy	DoD Cloud Computing Requirements Guide, Cloud Security Policy, Service Level Agreement

Analysis and sharing of assured software (COTS, GOTS, and Open Source)

PPP Outline & Guidance Approach:

- Recognizes the importance of software reuse to deliver at the speed of relevance.
- Incorporates the identification of vendor best practices to mitigate risks identified by EO 14028 Improving the Nation's Cybersecurity
- Enables validation and inheritance of vendor applied protections
- Informs selection of additional protections based on criticality and residual risks associated with provided vendor practices.

Program Protection Plan Outline and Guidance
Software Procurement (Notional Examples)

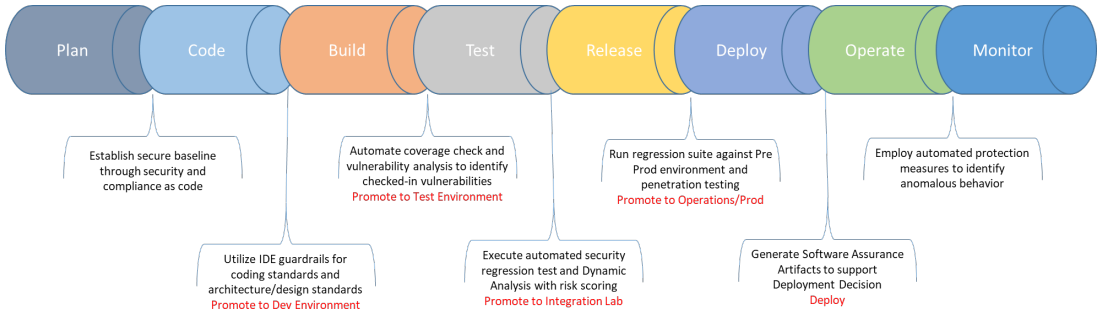
Scope	Development Vendor Technique(s) Applied	Procurement/Transition PMO / Contractor Technique(s) Applied	Organization(s) and or Vendor	References
Vendor A Component A	Vendor Secure Development Lifecycle, SBOM	Binary Analysis, Penetration Testing Supply Chain Illumination	Vendor A	vendor website Assessment #1
S&T Component A	Code Review, SAST, DAST	Penetration Testing	SEI	SEI Secure Coding SEI SDP
SCO 3	SSDF, Unit Test, SAST, SBOM	Binary Analysis (TT 5)	Contractor B	Contractor SDP, Test Process, Product SW Bill of Materials (SBOM)

*COTS: Commercial –off-the-shelf
GOTS: Government off the shelf

Establishing SwA thresholds for promotion of software

PPP O&G Approach:

- Categorizes vulnerabilities based on the software scope, assessment approach, and tool/technique used for analysis
- Enables PMO to establish acceptance thresholds based on the environment and criticality of the software
- Supports continuous integration and testing at all stages of the software lifecycle
- Informs decision makers of latent vulnerabilities, maturation of acceptance thresholds, and assurance trends based on vulnerability scoring



Program Protection Plan Outline and Guidance
Software Weaknesses and Vulnerabilities (Notional Examples)

Software Scope ID (Table 9-3)	Techniques and Tools (Table 9-5)	Assessment Approach	Vulnerability Scoring	Acceptance Thresholds	Report (ID)
SCO 1	TT 2	Daily Scan and Reports	Tool Generated	No Critical or High in Prod	Report A (SWR 1)
SCO 2	TT 1	Automated scanning of binary	CVSS	Mitigations for all findings > 6.9	Report B (SWR 2)
SCO 3	TT 3	All code check-in	N/A (Coverage)	Mitigated prior to code commit	Report C (SWR 3)
SCO 2	TT 5	As needed based on findings from TT 1	Manual	All findings mitigated	Report B (SWR 4)

Promote use of Modern Software Frameworks, Technologies and Languages

PPP Outline & Guidance Approach:

- Recognizes the importance of innovation and protections that can be achieved through selection of modern capabilities
- Enables PMO to reference or summarize software development processes, frameworks and standards being used to highlight assurance best practices
- Encourages the use of modern technologies, reference designs, and development languages to enhance assurance
- Informs, through mapping to the software scope, assurance gaps based on residual risks

Software Scope (Notional Examples)

Software Scope ID for PPP Trace-ability	Software Description	Software Type	Developer(s)
SCO 1	CSCI #1	Application	Contractor A, B, & C
SCO 2	Critical Function #1	Application	Government Program Mana
SCO 3	Critical Component #1	Embedded	Contr
SCO 4	Critical Component #2	Application	Open

Software Process Summary (Notional Examples)

Topic	Summary	Software ID for PPP Traceability	References
Software and Firmware Development, Procurement, Verification	Software Development process is described in the SDP. Development pipeline employs software composition analysis, source code analysis, two level code review, dynamic analysis, and automated test scripts for security. Practices identified as part of verification are included in the software test plan.	SCO 1 SCO 2 SCO 3	SDP X.X Test Plan X.X
	he lead integrator employs strict configuration anagement for all integrated and deployed ftware. Contractor CM supports full ceability from requirements through delivery. ystem employs configuration as code to sure secure deployment.	SCO 1 SCO 2 SCO 3 SCO 4	SDP X.X,
	ystem is being developed using the Major apability Acquisition Pathway. Subsystem A, C will utilize the SW Acquisition Pathway. onsiderations are included in the Acquisition rategy.	SCO 1 SCO2 SCO 3	Acquisition Strategy X.X

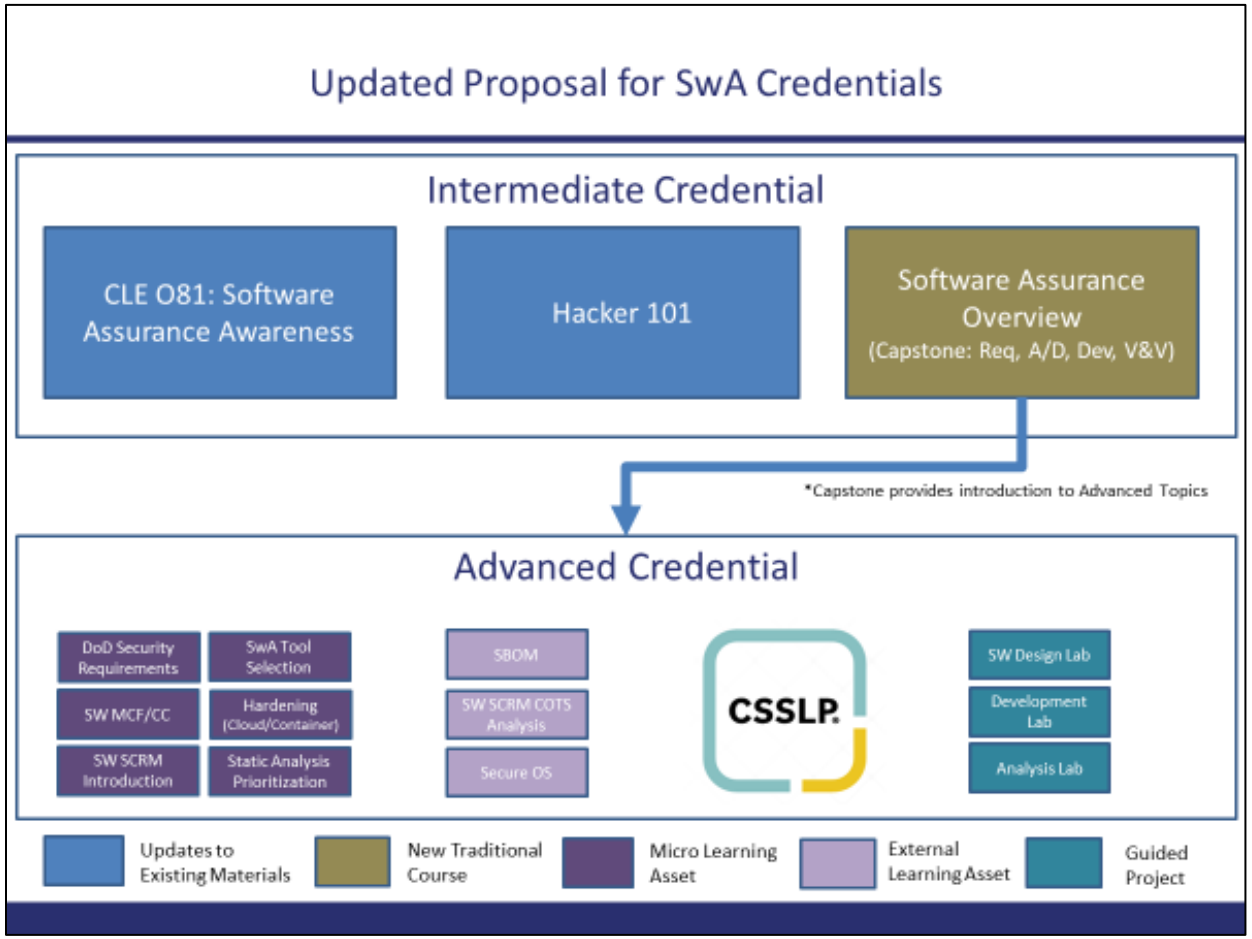
Software Protections (Notional Examples)

Design Selection & Category	Category	Inherent Protection Gained	Supplemental Protection Required	Software Scope Applied	References
NIST SSDF	Standards	N/A	N/A	SCO 1-3	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
DoD DevSecOps Reference Design	D&A	Service Mesh with security sidecar	Additional Protections applied at the application layer	SCO 1	https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
Rust programming language	Language	Memory safe language Null Pointer Safety Data Race Safety	Code Review (TT 3)	SCO 4	N/A

Advance the SwA workforce through DAU SwA Credential Program

PPP Outline & Guidance Approach:

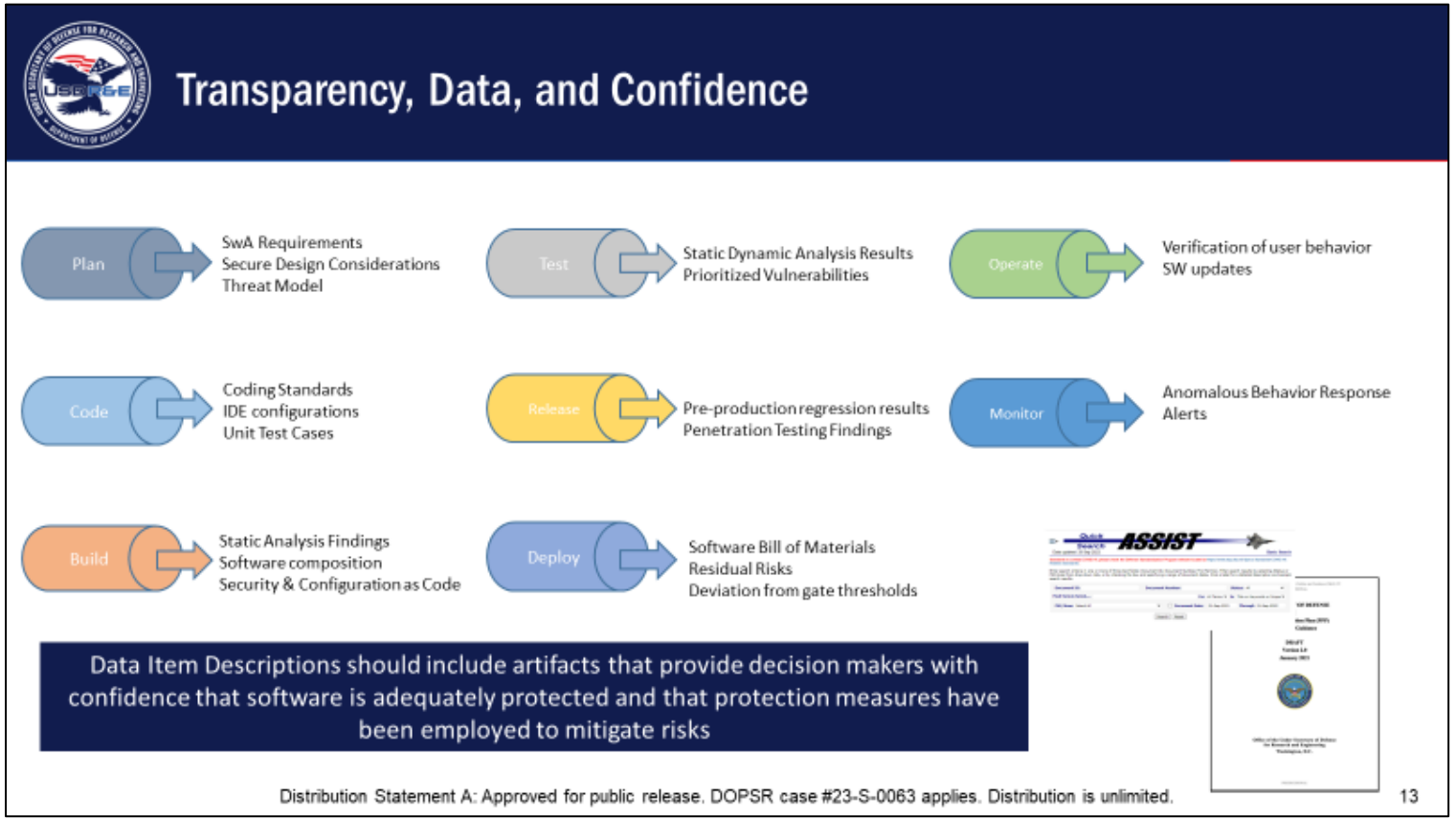
- Defense Acquisition University (DAU) is developing a SwA Credential Program with Intermediate and Advanced Credentials
- DAU plans to follow development of DevSecOps Credential Program leveraging Micro-learning assets, guided projects, and simulations.
- Focused on alignment with related competencies including Program Protection, Systems Engineering, and Software Development
- Intermediate Credential will provide overview of SwA responsibilities
- Advanced will review specific SwA methods and practices from various DoD roles



Advance the SwA Confidence Through Transparency and Data

Approach:

- Develop Data Identification Description that informs transparency into modern development pipelines and shared services
- Leverage existing software acquisition data to inform software protections and inform risk mitigations
- Encourage effective communication of SwA baselines and thresholds to reduce effort required for validation of findings
- Support the continuous evaluation of SwA posture and improvement trends throughout the development lifecycle



Summary

- **PPP O&G update to enable programs to identify, prioritize and implement modern software services, frameworks, and tools**

- **Automated collection and analysis of software assurance data is key to establishing and maintaining a SwA posture, commensurate with technology, program, system, and mission objectives.**

- **Key data elements include:**
  - Infrastructure and Platform security features that may be inherited through the use of shared services
  - Tools used in contractor pipelines across development, test, and production environments.
  - Artifacts generated through the application of SwA techniques in the development or integration of procured software
  - Modern development frameworks and processes that improve the assurance posture of the software being developed.

- **Industry support, review, and feedback on Program Protection DID(s) are 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