USD(R&E)

Software Assurance Roadmap Update

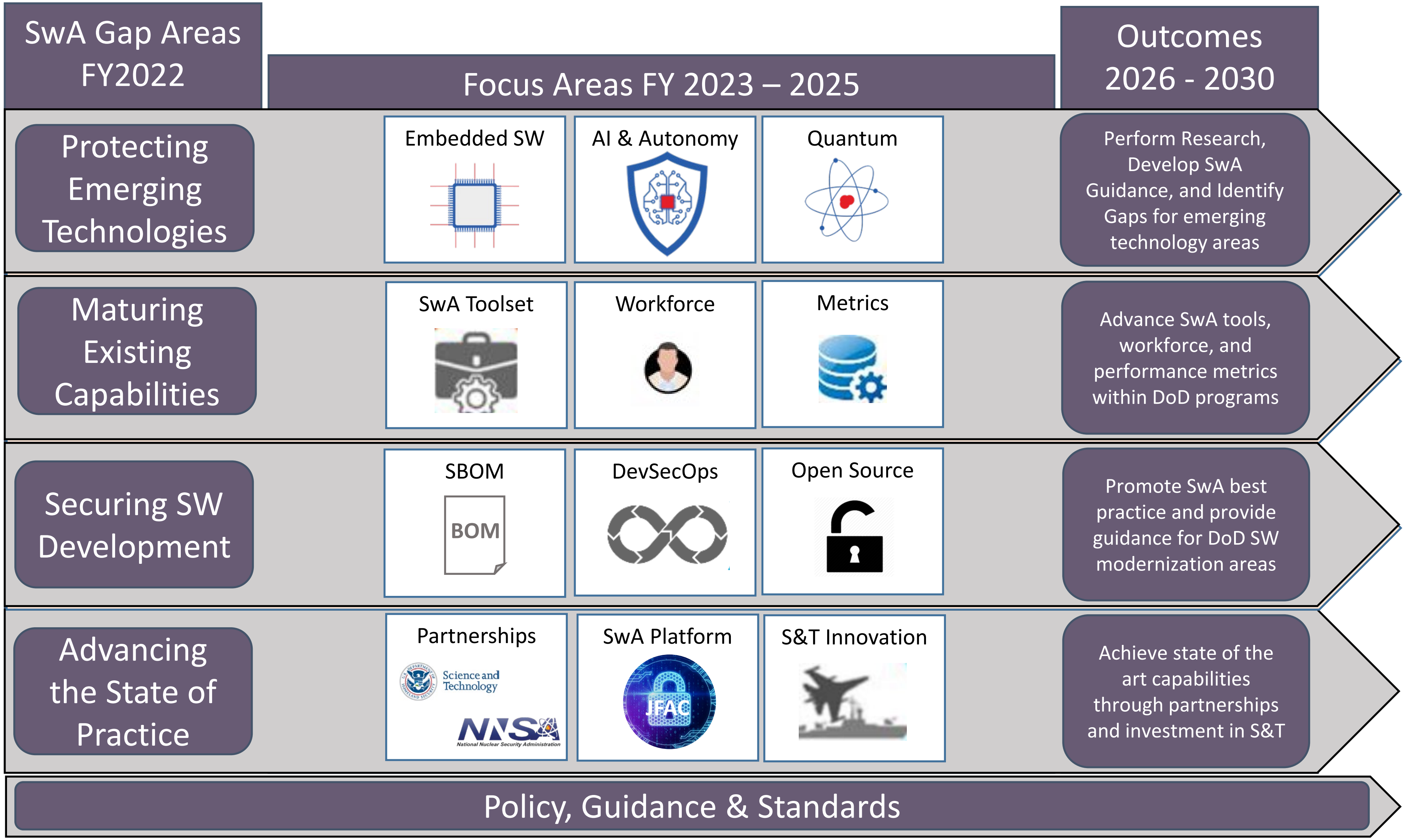
October 19, 2022

Bradley Lanford
SAIC Contractor Support
OUSD(R&E) S&TPP, Program Protection

Washington, DC

Distribution A. Approved for Public Release

Software Assurance Roadmap

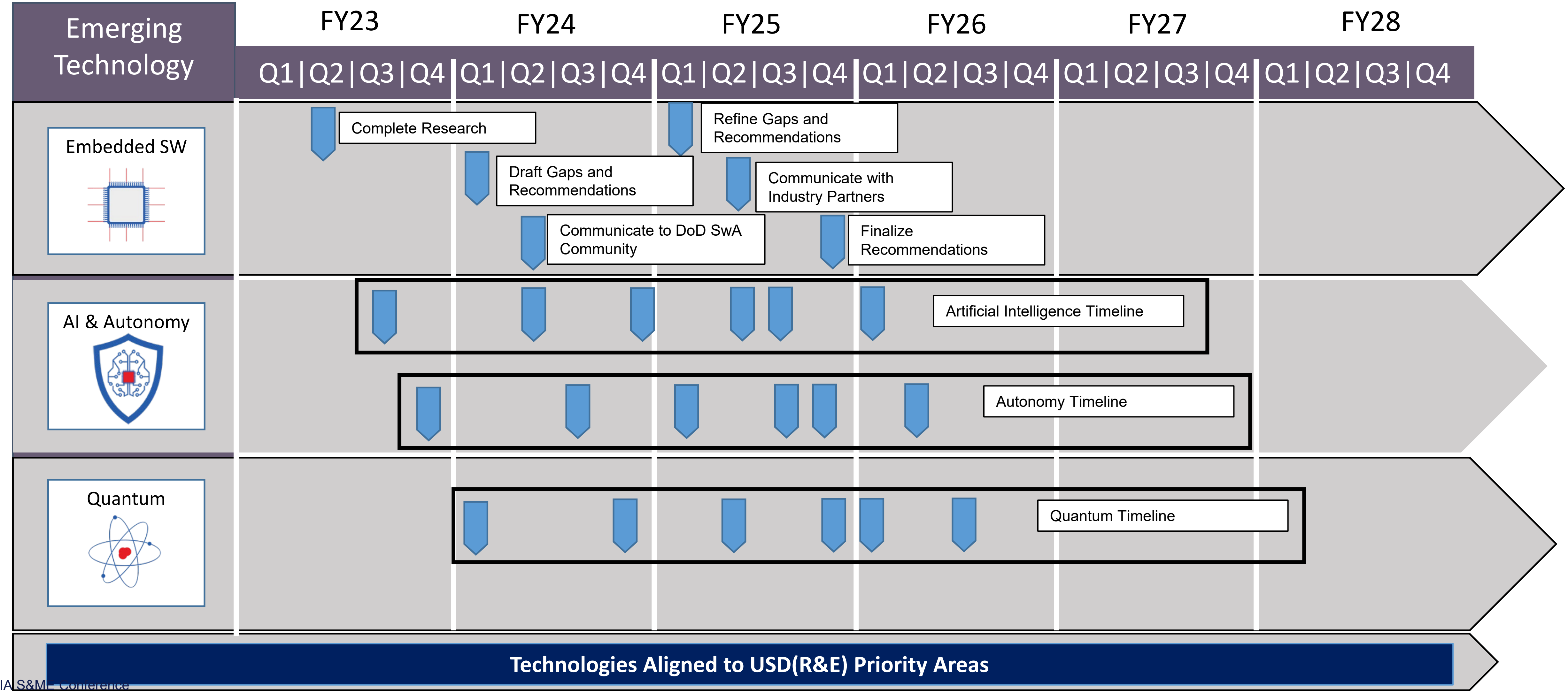


SwA Gap Areas FY2022	Focus Areas FY 2023 – 2025			Outcomes 2026 - 2030
Protecting Emerging Technologies	Embedded SW	AI & Autonomy	Quantum	Perform Research, Develop SwA Guidance, and Identify Gaps for emerging technology areas
Maturing Existing Capabilities	SwA Toolset	Workforce	Metrics	Advance SwA tools, workforce, and performance metrics within DoD programs
Securing SW Development	SBOM	DevSecOps	Open Source	Promote SwA best practice and provide guidance for DoD SW modernization areas
Advancing the State of Practice	Partnerships	SwA Platform	S&T Innovation	Achieve state of the art capabilities through partnerships and investment in S&T
Policy, Guidance & Standards				

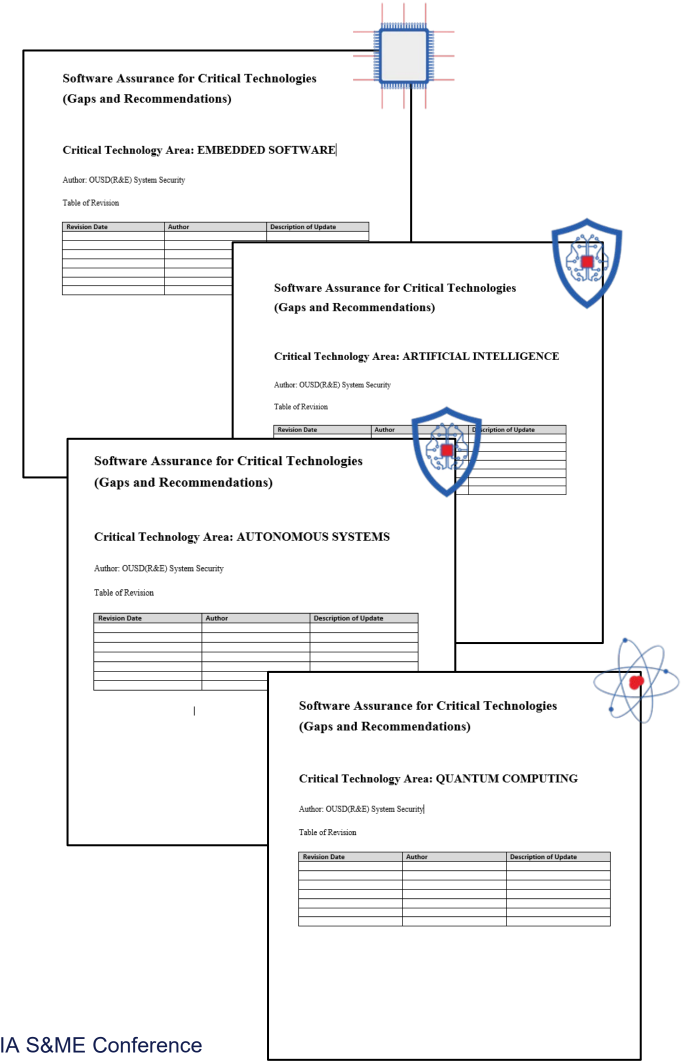
NDIA S&ME Conference
Oct 16-19, 2023

Distribution A. Approved for Public Release

Software Assurance Roadmap
Emerging Technologies


Emerging Technology
FY23
FY24
FY25
FY26
FY27
FY28
Q1|Q2|Q3|Q4|Q1|Q2|Q3|Q4|Q1|Q2|Q3|Q4|Q1|Q2|Q3|Q4|Q1|Q2|Q3|Q4|Q1|Q2|Q3|Q4
Embedded SW
Complete Research
Draft Gaps and Recommendations
Communicate to DoD SwA Community
Refine Gaps and Recommendations
Communicate with Industry Partners
Finalize Recommendations
AI & Autonomy
Artificial Intelligence Timeline
Autonomy Timeline
Quantum
Quantum Timeline
Technologies Aligned to USD(R&E) Priority Areas

Software Assurance Roadmap Emerging Technologies



Software Assurance for Critical Technologies (Gaps and Recommendations)

Critical Technology Area: EMBEDDED SOFTWARE

Author: OUSD(R&E) System Security

Table of Revision

Revision Date	Author	Description of Update

Software Assurance for Critical Technologies (Gaps and Recommendations)

Critical Technology Area: ARTIFICIAL INTELLIGENCE

Author: OUSD(R&E) System Security

Table of Revision

Revision Date	Author	Description of Update

Software Assurance for Critical Technologies (Gaps and Recommendations)

Critical Technology Area: AUTONOMOUS SYSTEMS

Author: OUSD(R&E) System Security

Table of Revision

Revision Date	Author	Description of Update

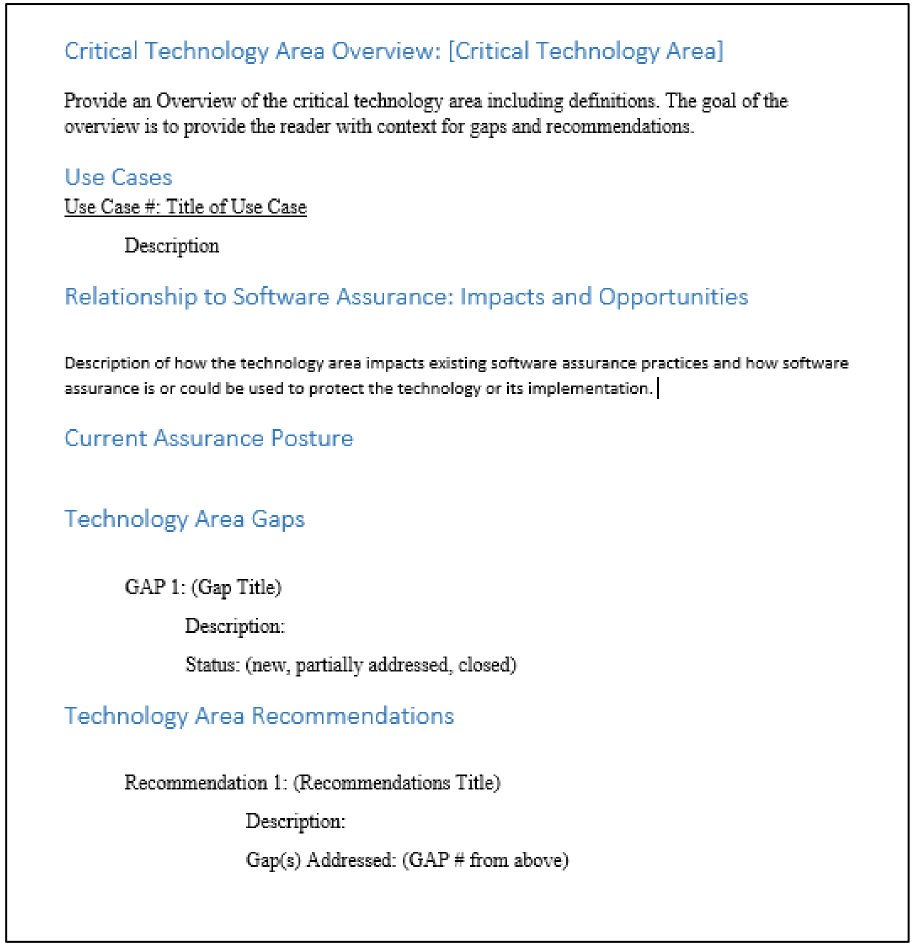
Software Assurance for Critical Technologies (Gaps and Recommendations)

Critical Technology Area: QUANTUM COMPUTING

Author: OUSD(R&E) System Security

Table of Revision

Revision Date	Author	Description of Update



Critical Technology Area Overview: [Critical Technology Area]

Provide an Overview of the critical technology area including definitions. The goal of the overview is to provide the reader with context for gaps and recommendations.

Use Cases

Use Case #: Title of Use Case

Description

Relationship to Software Assurance: Impacts and Opportunities

Description of how the technology area impacts existing software assurance practices and how software assurance is or could be used to protect the technology or its implementation.

Current Assurance Posture

Technology Area Gaps

GAP 1: (Gap Title)

Description:

Status: (new, partially addressed, closed)

Technology Area Recommendations

Recommendation 1: (Recommendations Title)

Description:

Gap(s) Addressed: (GAP # from above)

Example Gap / Recommendations

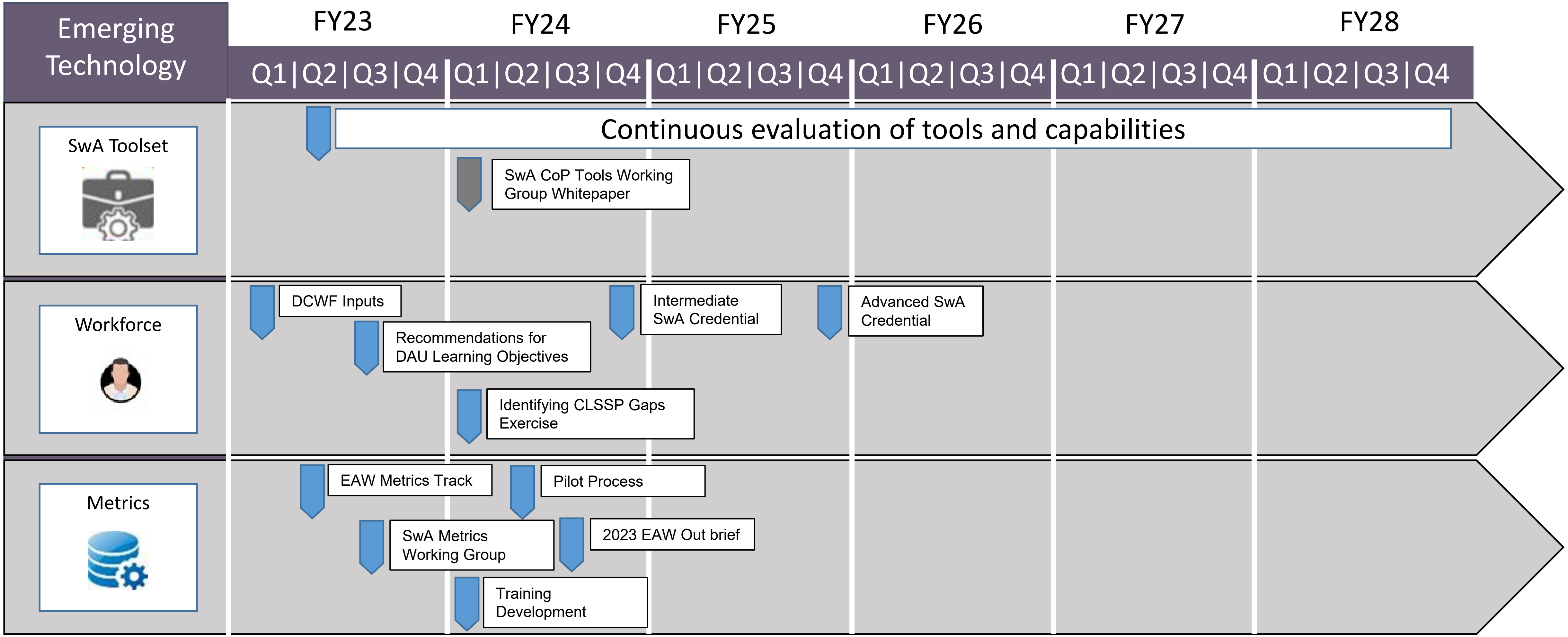
GAP 1: Lack of Ethical Hacking Resources

Description: Due to the custom aspects of embedded software developed and used by the DoD, the constraints on our ability to analyze legacy software and ineffectiveness of many commercial tools in the embedded domain, ethical hacking may be our best alternative. Creating and fostering a community of ethical hackers could be beneficial in helping industry improve their security posture. Introducing ethical hacking in the software lifecycle should provide software engineers with real-time feedback, helping them think like hackers as they ship code.

Recommendation 1: Invest in and make available ethical hacking training across different form factors of embedded software.

Recommendation 2: Automate discovery of common malicious features across embedded software form factors to reduce manual evaluation

Software Assurance Roadmap
Maturing Existing Capabilities



Emerging Technology

FY23 | FY24 | FY25 | FY26 | FY27 | FY28

Q1|Q2|Q3|Q4 | Q1|Q2|Q3|Q4 | Q1|Q2|Q3|Q4 | Q1|Q2|Q3|Q4 | Q1|Q2|Q3|Q4 | Q1|Q2|Q3|Q4

SwA Toolset

Continuous evaluation of tools and capabilities

SwA CoP Tools Working Group Whitepaper

Workforce

DCWF Inputs

Recommendations for DAU Learning Objectives

Identifying CLSSP Gaps Exercise

Intermediate SwA Credential

Advanced SwA Credential

Metrics

EAW Metrics Track

SwA Metrics Working Group

Training Development

Pilot Process

2023 EAW Out brief

Acronyms

SwA CoP: Software Assurance Community of Practice

CLSSP: Certified Secure Software Lifecycle Professional

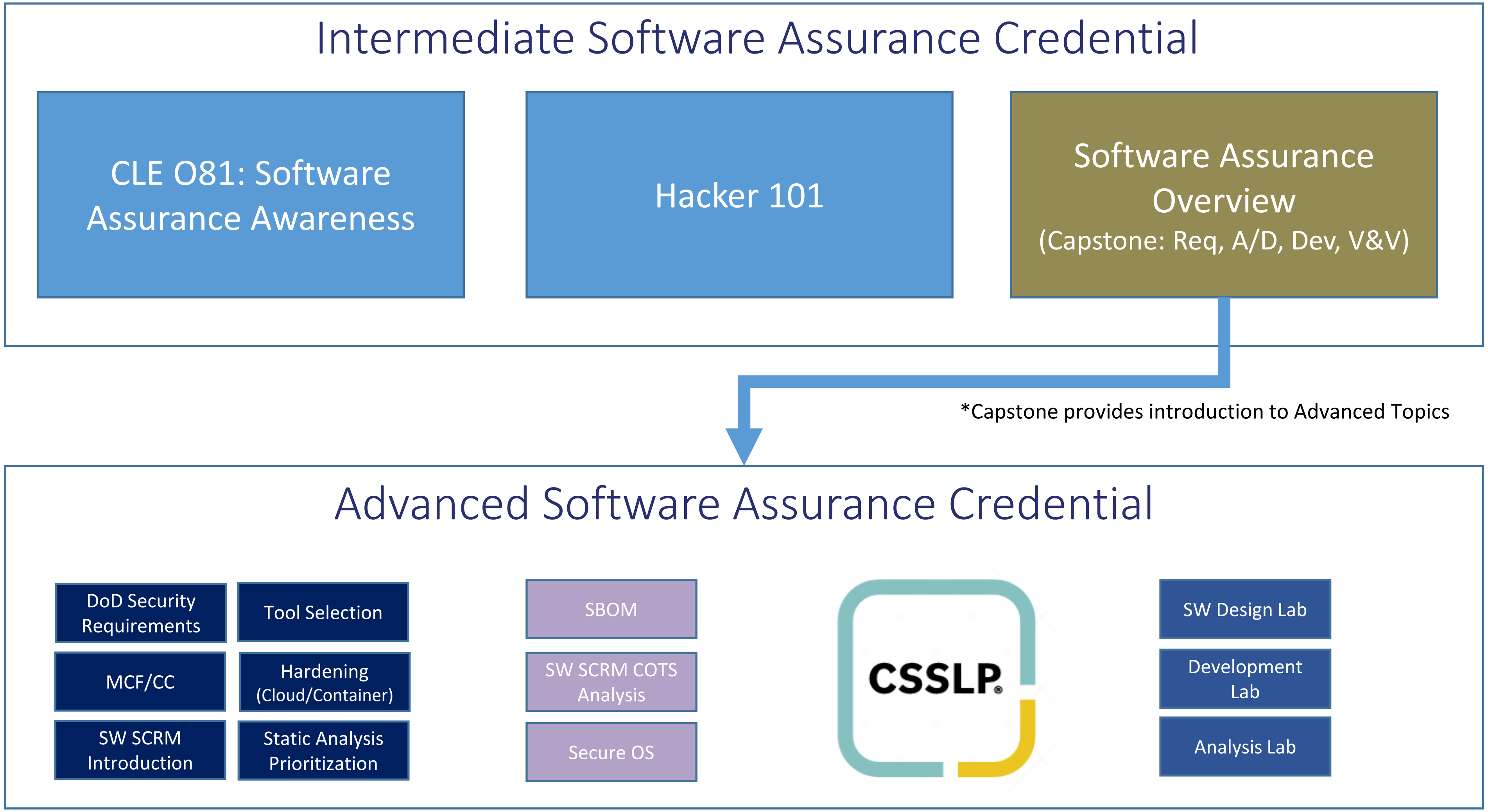
DCWF: Defense Cyber Workforce

EAW: Enterprise Assurance Workshop

🟦 OUSD(R&E) SwA effort

⬛ External effort

Software Assurance Roadmap Workforce



Intermediate Software Assurance Credential

CLE O81: Software Assurance Awareness

Hacker 101

Software Assurance Overview (Capstone: Req, A/D, Dev, V&V)

*Capstone provides introduction to Advanced Topics

Advanced Software Assurance Credential

DoD Security Requirements

Tool Selection

MCF/CC

Hardening (Cloud/Container)

SW SCRM Introduction

Static Analysis Prioritization

SBOM

SW SCRM COTS Analysis

Secure OS

CSSLP

SW Design Lab

Development Lab

Analysis Lab

🟦 Updates to Existing Materials

▨ New Traditional Course

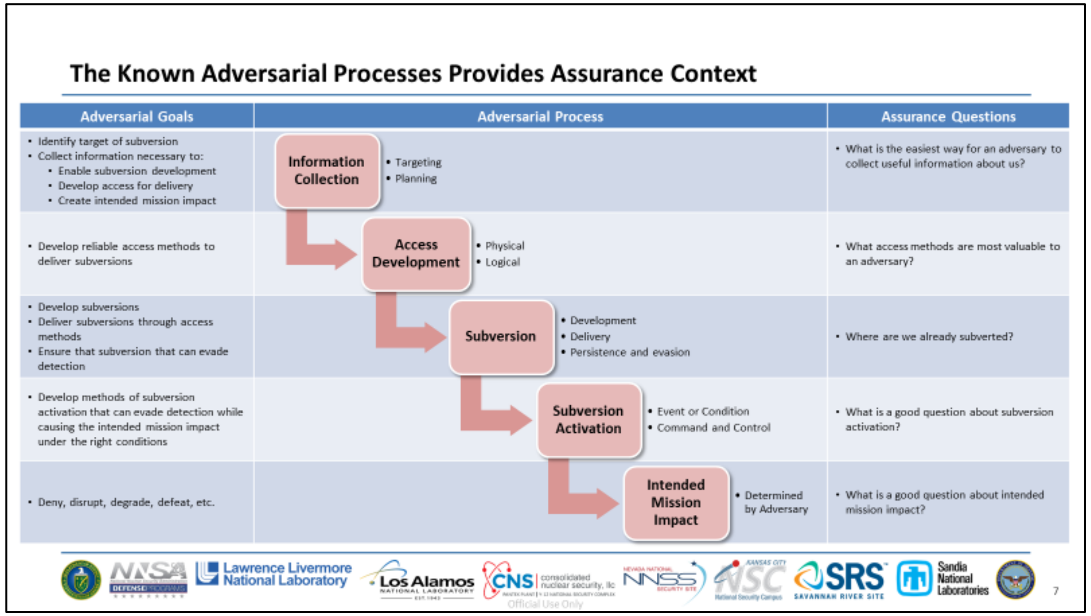
■ Micro Learning Asset

🟨 External Learning Asset

🟦 Guided Project

Acronyms
A/D: Architecture and Design
Req: Requirements
Dev: Development
V&V: Verification and Validation
SwA CoP: Software Assurance Community of Practice
CLSSP: Certified Secure Software Lifecycle Professional
MCF: Mission Critical Function
CC: Critical Components
SCRM: Supply Chain Risk Management
SBOM: Software Bill of Materials
COTS: Commercial Off the Shelf

Software Assurance Roadmap
Metrics

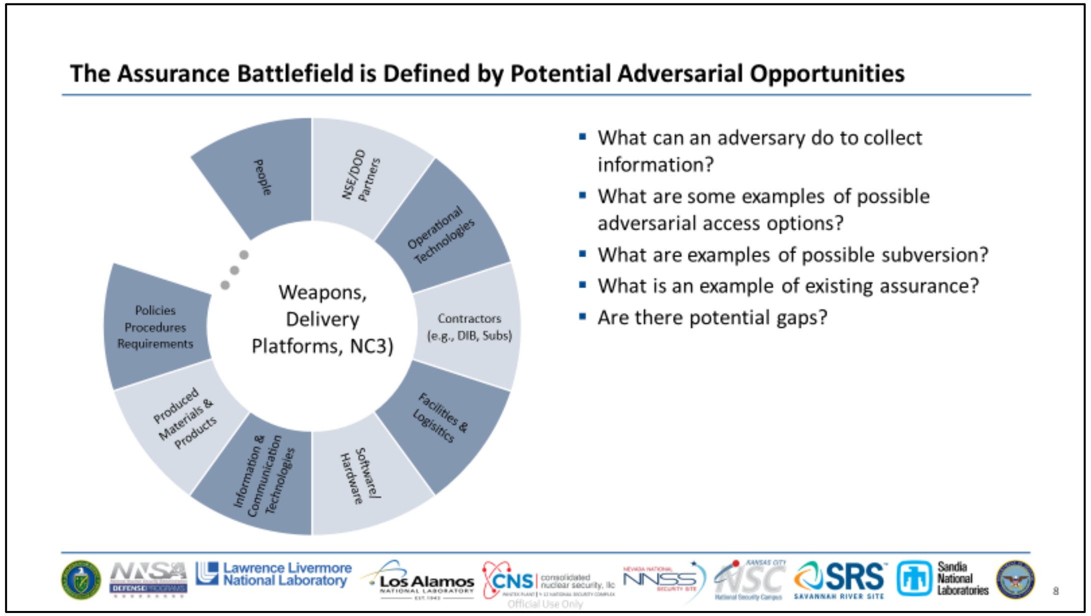


The Known Adversarial Processes Provides Assurance Context

Adversarial Goals	Adversarial Process		Assurance Questions
• Identify target of subversion • Collect information necessary to: • Enable subversion development • Develop access for delivery • Create intended mission impact	Information Collection	• Targeting • Planning	• What is the easiest way for an adversary to collect useful information about us?
• Develop reliable access methods to deliver subversions	Access Development	• Physical • Logical	• What access methods are most valuable to an adversary?
• Develop subversions • Deliver subversions through access methods • Ensure that subversion that can evade detection	Subversion	• Development • Delivery • Persistence and evasion	• Where are we already subverted?
• Develop methods of subversion activation that can evade detection while causing the intended mission impact under the right conditions	Subversion Activation	• Event or Condition • Command and Control	• What is a good question about subversion activation?
• Deny, disrupt, degrade, defeat, etc.	Intended Mission Impact	• Determined by Adversary	• What is a good question about intended mission impact?

Official Use Only

7



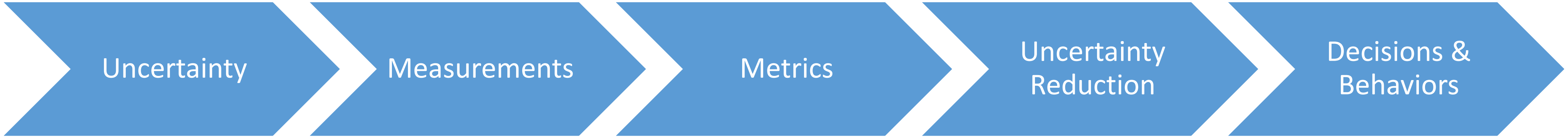
The Assurance Battlefield is Defined by Potential Adversarial Opportunities

Weapons, Delivery Platforms, NC3)
People
NSE/DOD Partners
Operational Technologies
Contractors (e.g., DIB, Subs)
Facilities & Logisitics
Software/ Hardware
Information & Communication Technologies
Produced Materials & Products
Policies Procedures Requirements

- What can an adversary do to collect information?
- What are some examples of possible adversarial access options?
- What are examples of possible subversion?
- What is an example of existing assurance?
- Are there potential gaps?

Official Use Only

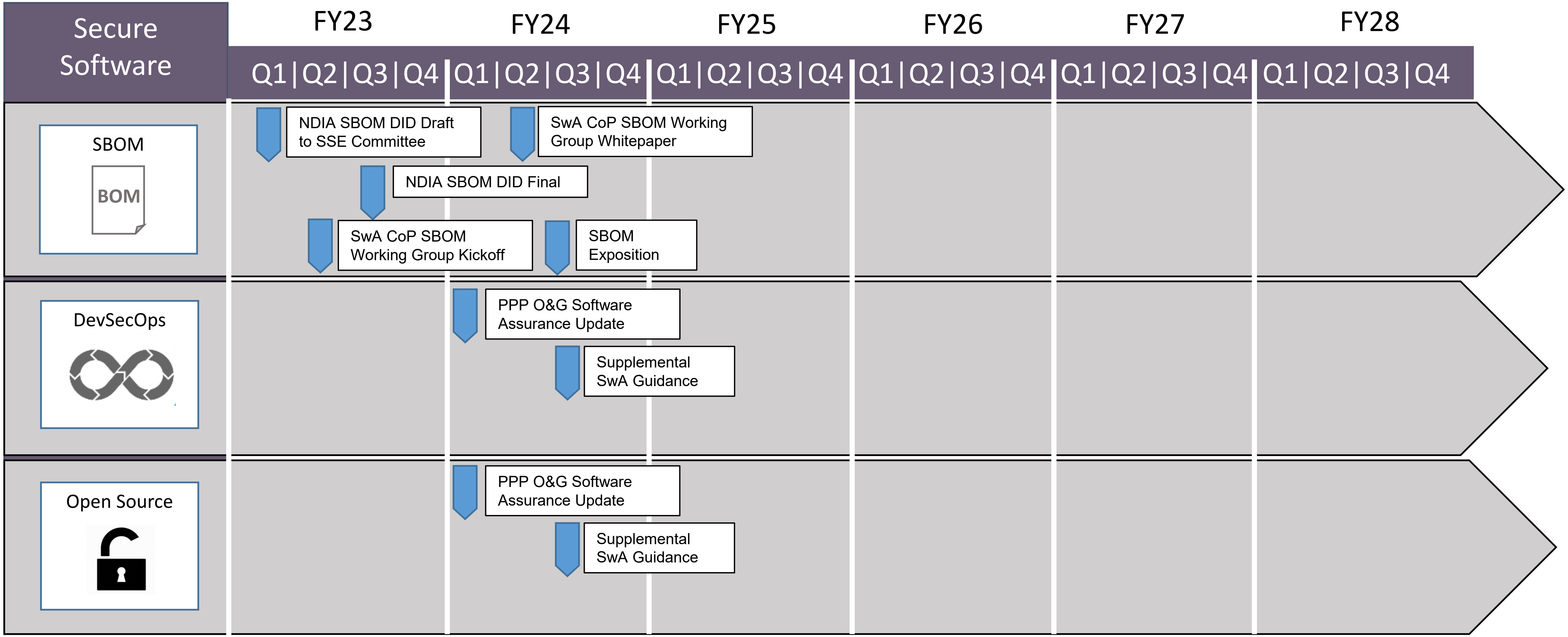
8



Software Assurance Community is using exercises defined at 2022 Nuclear Enterprise Assurance Workshop to exercise metrics development process. Process is based on defining adversarial opportunities based on the steps of the adversarial process. Next steps are to develop training materials to support pilot.

Distribution A. Approved for Public Release

Software Assurance Roadmap
Maturing Existing Capabilities



Secure Software

FY23 FY24 FY25 FY26 FY27 FY28

Q1|Q2|Q3|Q4 Q1|Q2|Q3|Q4 Q1|Q2|Q3|Q4 Q1|Q2|Q3|Q4 Q1|Q2|Q3|Q4 Q1|Q2|Q3|Q4

SBOM

BOM

NDIA SBOM DID Draft to SSE Committee

SwA CoP SBOM Working Group Whitepaper

NDIA SBOM DID Final

SwA CoP SBOM Working Group Kickoff

SBOM Exposition

DevSecOps

PPP O&G Software Assurance Update

Supplemental SwA Guidance

Open Source

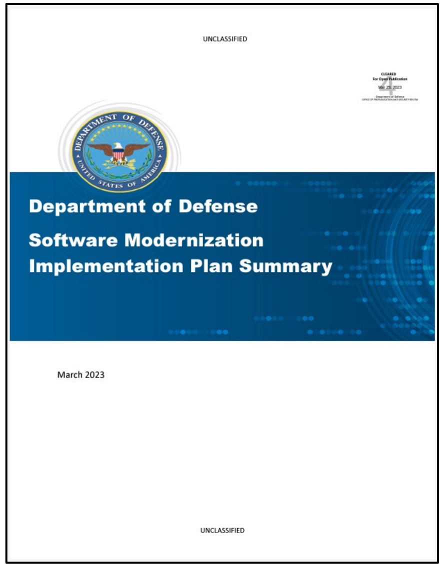
PPP O&G Software Assurance Update

Supplemental SwA Guidance

Acronyms
NDIA: National Defense Industrial Association
DID: Data Item Description
PPP O&G: Program Protection Plan Outline and Guidance

Distribution A. Approved for Public Release

Software Assurance Roadmap
Software Modernization


UNCLASSIFIED

CLEARED
For Open Publication

Mar 29, 2023

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

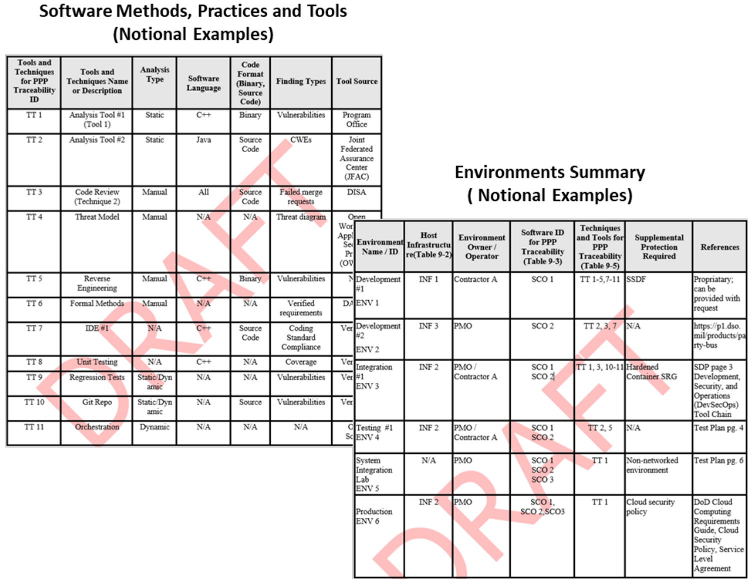
Department of Defense

Software Modernization Implementation Plan Summary

March 2023

UNCLASSIFIED

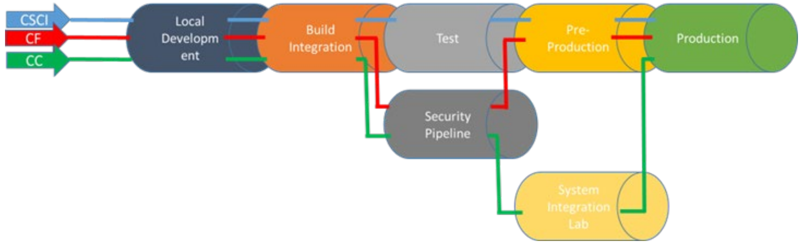
- Inheritance of assurance through adoption of infrastructure and platforms
- Integration of assurance tools into DoD Software factory pipelines
- Analysis and sharing of assured software (COTS, GOTS, and Open Source)
- Establishing SwA thresholds for promotion of software
- Promote the use of modern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


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 Appl Se Pr (OW
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

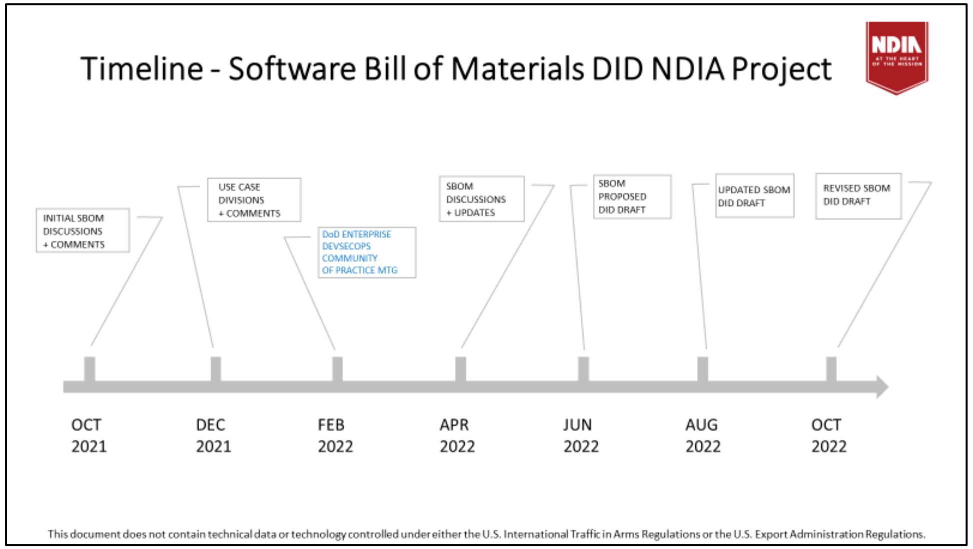
Environments Summary
(Notional Examples)

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



Software Assurance Roadmap
Software Bill of Materials

National Defense Industrial Association

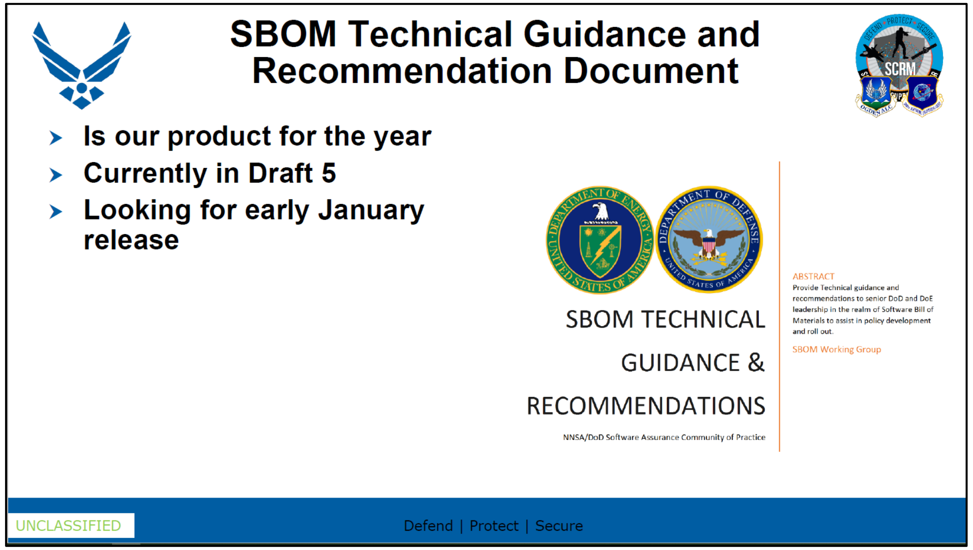


Timeline - Software Bill of Materials DID NDIA Project

NDIA
AT THE HEART OF THE MISSION
INITIAL SBOM DISCUSSIONS + COMMENTS
USE CASE DIVISIONS + COMMENTS
DoD ENTERPRISE DEVSECOPS COMMUNITY OF PRACTICE MTG
SBOM DISCUSSIONS + UPDATES
SBOM PROPOSED DID DRAFT
UPDATED SBOM DID DRAFT
REVISED SBOM DID DRAFT
OCT 2021
DEC 2021
FEB 2022
APR 2022
JUN 2022
AUG 2022
OCT 2022

This document does not contain technical data or technology controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Software Assurance Community of Practice



SBOM Technical Guidance and Recommendation Document

- Is our product for the year
- Currently in Draft 5
- Looking for early January release

SBOM TECHNICAL GUIDANCE & RECOMMENDATIONS

NNSA/DoD Software Assurance Community of Practice

ABSTRACT

Provide Technical guidance and recommendations to senior DoD and DoE leadership in the realm of Software Bill of Materials to assist in policy development and roll out.

SBOM Working Group

UNCLASSIFIED

Defend | Protect | Secure

Partnerships

CISA — Cybersecurity & Infrastructure Security Agency

NNSA — National Nuclear Security Administration

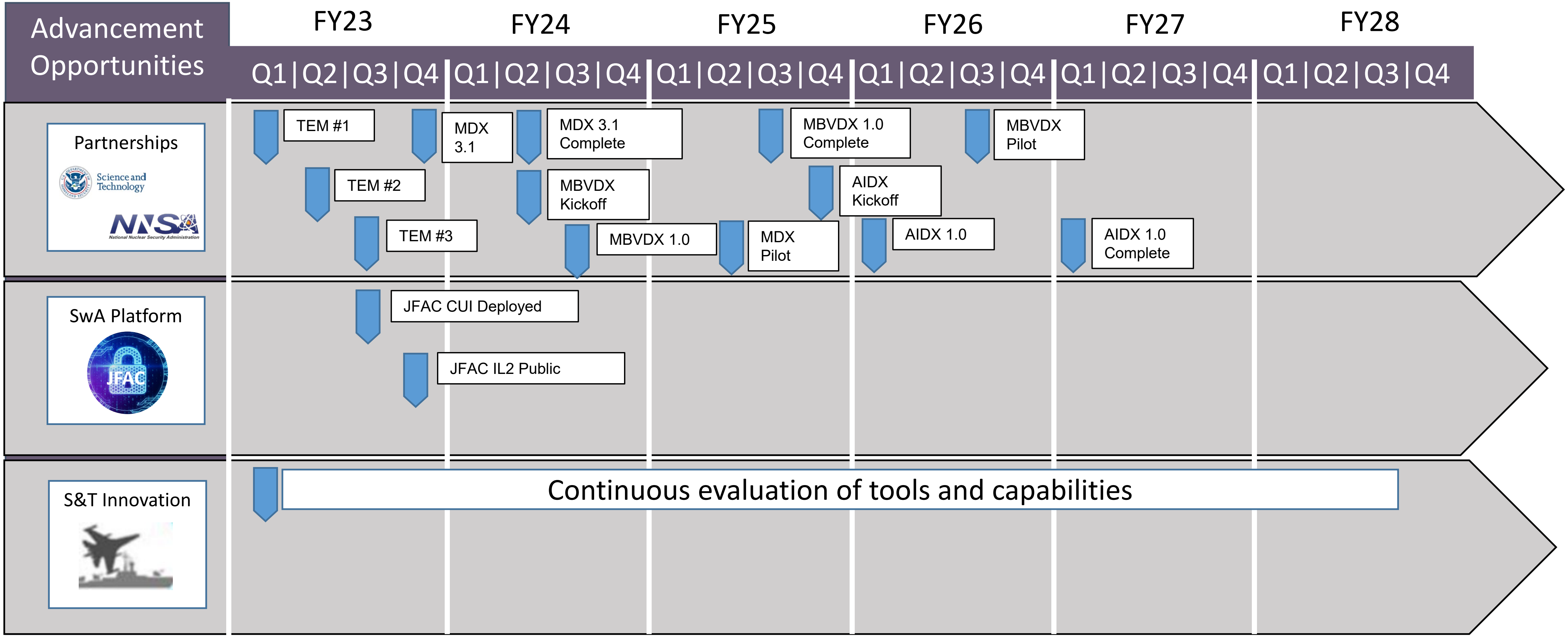
CDAO — Chief Digital and Artificial Intelligence Office

Department of Defense Chief Information Officer

Informing implementation of EO 14028 through partnerships with the Interagency, DoD Stakeholders, and Industry

Distribution A. Approved for Public Release

Software Assurance Roadmap
Maturing Existing Capabilities



Advancement Opportunities

FY23 Q1|Q2|Q3|Q4 FY24 Q1|Q2|Q3|Q4 FY25 Q1|Q2|Q3|Q4 FY26 Q1|Q2|Q3|Q4 FY27 Q1|Q2|Q3|Q4 FY28 Q1|Q2|Q3|Q4

Partnerships

TEM #1

TEM #2

TEM #3

MDX 3.1

MDX 3.1 Complete

MBVDX Kickoff

MBVDX 1.0

MDX Pilot

MBVDX 1.0 Complete

AIDX Kickoff

AIDX 1.0

MBVDX Pilot

AIDX 1.0 Complete

SwA Platform

JFAC CUI Deployed

JFAC IL2 Public

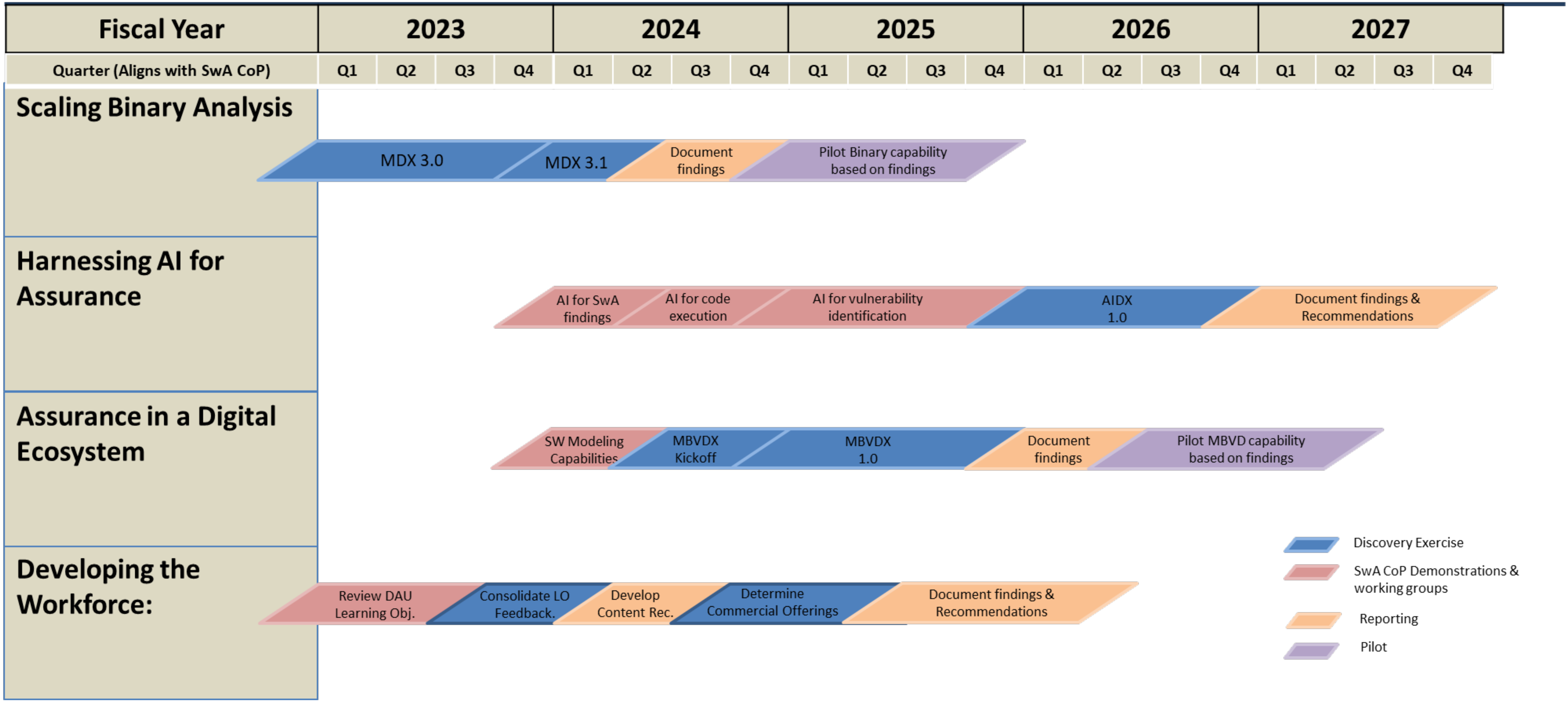
S&T Innovation

Continuous evaluation of tools and capabilities

Acronyms
TEM: Technical Exchange Meeting
MDX: Malware Discovery Exercise
MBVDX: Model Based Vulnerability Discovery Exercise
AIDX: Artificial Intelligence Discovery Exercise
JFAC: Joint Federated Assurance Center
CUI: Controlled Unclassified Information
IL: Impact Level

Distribution A. Approved for Public Release

Software Assurance Roadmap Partnerships



Fiscal Year: 2023, 2024, 2025, 2026, 2027

Quarter (Aligns with SwA CoP): Q1, Q2, Q3, Q4 for each year

Scaling Binary Analysis

- MDX 3.0
- MDX 3.1
- Document findings
- Pilot Binary capability based on findings

Harnessing AI for Assurance

- AI for SwA findings
- AI for code execution
- AI for vulnerability identification
- AIDX 1.0
- Document findings & Recommendations

Assurance in a Digital Ecosystem

- SW Modeling Capabilities
- MBVDX Kickoff
- MBVDX 1.0
- Document findings
- Pilot MBVD capability based on findings

Developing the Workforce:

- Review DAU Learning Obj.
- Consolidate LO Feedback.
- Develop Content Rec.
- Determine Commercial Offerings
- Document findings & Recommendations

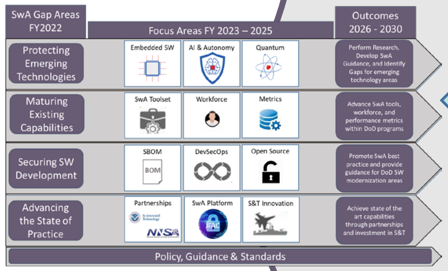
🟦 Discovery Exercise

🟥 SwA CoP Demonstrations & working groups

🟧 Reporting

🟪 Pilot

Software Assurance Roadmap
Joint Federated Assurance Center Platform



SwA Gap Areas FY2022 | Focus Areas FY 2023 – 2025 | Outcomes 2026 - 2030

Protecting Emerging Technologies — Embedded SW, AI & Autonomy, Quantum — Perform Research, Develop SwA Guidance, and Identify Gaps for emerging technology areas

Maturing Existing Capabilities — SwA Toolset, Workforce, Metrics — Advance SwA tools, workforce, and performance metrics within DoD programs

Securing SW Development — SBOM, DevSecOps, Open Source — Promote SwA best practice and provide guidance for DoD SW modernization areas

Advancing the State of Practice — Partnerships, SwA Platform, S&T Innovation — Achieve state of the art capabilities through partnerships and investment in S&T

Policy, Guidance & Standards

Enabling Technologies

Embedded SW | Quantum | AI & Autonomy

Technical Deliverables and identified best practices are shared with **JFAC leadership and the Technical Working Group (TWG)** to inform:

- Program Adoption of best practices
- JFAC investment in assurance capabilities and research

Existing Capabilities

Metrics | Workforce | SwA Toolset

- Tool Landscape studies are integrated into **JFAC-CSC** portal
- Collaboration with **JFAC TWG** to inform tool effectiveness, pilot SwA metrics and identify SwA training
- Inform **JFAC leadership** of gaps for investment

Secure SW Dev

Open Source | DevSecOps | SBOM

Technical Deliverables and identified best practices are shared with **JFAC leadership and TWG** to inform:

- Program Adoption of best practices
- JFAC investment in assurance capabilities and research

Advancement

Partnerships | S&T Innovation | SwA Platform

- Partnership with **JFAC Leadership** to support Joint SwA Roadmap
- S&T Landscape studies are integrated into **JFAC-CSC** portal
- Collaboration with **JFAC TWG** and **JFAC-CSC** to inform development of JFAC portal requirements
- Inform **JFAC leadership** of gaps for investment

JFAC

BUILDING TRUST THROUGH HOLISTIC ASSURANCE

JFAC - CSC:

Questions?

Bradley Lanford

SAIC Contractor Support

Office of the Under Secretary of Defense
for Research and Engineering

bradley.p.lanford.ctr@mail.mil