USD(R&E)

Software Assurance Roadmap

Mr. Steve Grice
Technical Director, Software Assurance

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

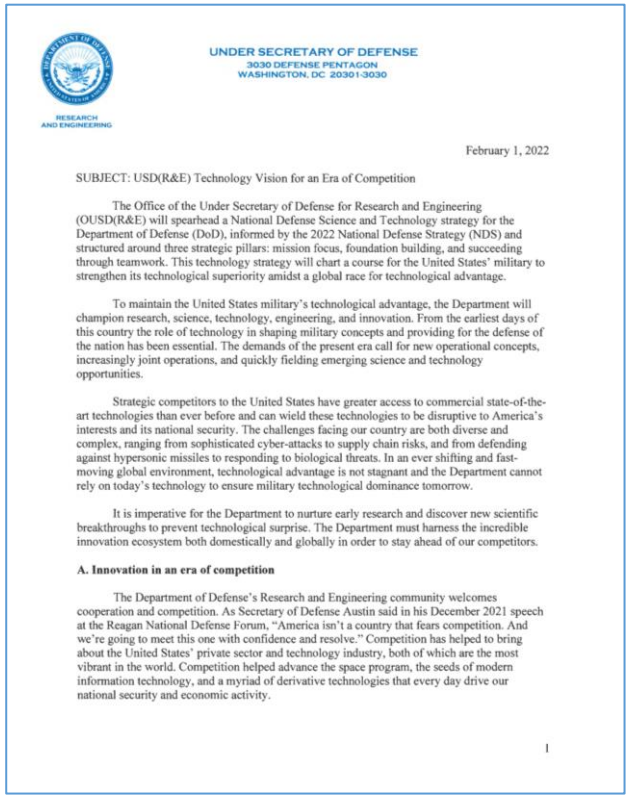
Software Assurance

- **Software Assurance (SwA):**
  - *The level of confidence that software functions only as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle*
    - PL112–239, JAN. 2, 2013, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, Section 933

- **Activities to Date**
  - Development of policies, instructions, guides, and standards to promote best practices
  - Joint Federated Assurance Center (JFAC)
  - JFAC Technical Working Group Community
  - DoD/National Nuclear Security Administration (NNSA) Software Assurance Community of Practice
  - Partnerships with Department of Homeland Security, NNSA, National Security Agency, and Industry thru NDIA

Strategic Vision

Ms. Heidi Shyu, Under Secretary of Defense for Research and Engineering, released *"Technology Vision for an Era of Competition,"* (dated February 1, 2022) to provide guidance on those areas needing further technology investments.



UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH AND ENGINEERING

February 1, 2022

SUBJECT: USD(R&E) Technology Vision for an Era of Competition

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E) will spearhead a National Defense Science and Technology strategy for the Department of Defense (DoD), informed by the 2022 National Defense Strategy (NDS) and structured around three strategic pillars: mission focus, foundation building, and succeeding through teamwork. This technology strategy will chart a course for the United States' military to strengthen its technological superiority amidst a global race for technological advantage.

To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities.

Strategic competitors to the United States have greater access to commercial state-of-the-art technologies than ever before and can wield these technologies to be disruptive to America's interests and its national security. The challenges facing our country are both diverse and complex, ranging from sophisticated cyber-attacks to supply chain risks, and from defending against hypersonic missiles to responding to biological threats. In an ever shifting and fast-moving global environment, technological advantage is not stagnant and the Department cannot rely on today's technology to ensure military technological dominance tomorrow.

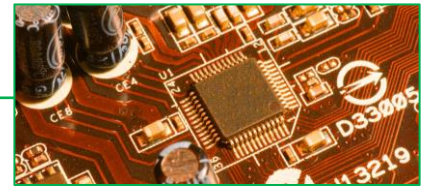
It is imperative for the Department to nurture early research and discover new scientific breakthroughs to prevent technological surprise. The Department must harness the incredible innovation ecosystem both domestically and globally in order to stay ahead of our competitors.

A. Innovation in an era of competition

The Department of Defense's Research and Engineering community welcomes cooperation and competition. As Secretary of Defense Austin said in his December 2021 speech at the Reagan National Defense Forum, "America isn't a country that fears competition. And we're going to meet this one with confidence and resolve." Competition has helped to bring about the United States' private sector and technology industry, both of which are the most vibrant in the world. Competition helped advance the space program, the seeds of modern information technology, and a myriad of derivative technologies that every day drive our national security and economic activity.

Strategic Vision *(continued)*

- **Critical Technology Areas**
  - Effective Adoption Areas
    - Trusted AI and Autonomy
    - Integrated Network Systems-of-Systems
    - Microelectronics
    - Space Technology
    - Renewable Energy Generation and Storage
    - Advance Computing and Software
    - Human-Machine Interfaces
  - Seed Areas of Emerging Opportunity
    - Biotechnology
    - Quantum Science
    - Future Generation Wireless Technology (FutureG)
    - Advance Materials
  - Defense-Specific Areas
    - Directed Energy
    - Hypersonics
    - Integrated Sensing and Cyber



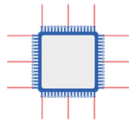
Strategic Vision *(continued)*

- **Current, Ongoing, and Relevant Topics**
  - Software Bill of Materials (SBOM)
    - Executive Order 14028, “Improving the Nation’s Cybersecurity”
    - FY19 NDAA Section 1655: Mitigation of risks from disclosure to foreign adversaries
    - Enduring Security Framework, Securing the Software Supply Chain
  - DevSecOps
    - DoD Instruction 5000.83, Technology and Program Protection, Program Protection Planning Outline and Guidance alignment with software modernization efforts
    - Identifying best practice for automation of SwA methods and practices
  - Existing Tool Maturation
    - Coordination with vendors, S&T organizations, and Service labs
    - PD Cyber and LLNL collaboration to evaluate tool landscape
  - Software Assurance Metrics
    - Development of metrics to support policy and guidance implementation
    - Nuclear Enterprise Assurance Workshop Metrics Track

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				

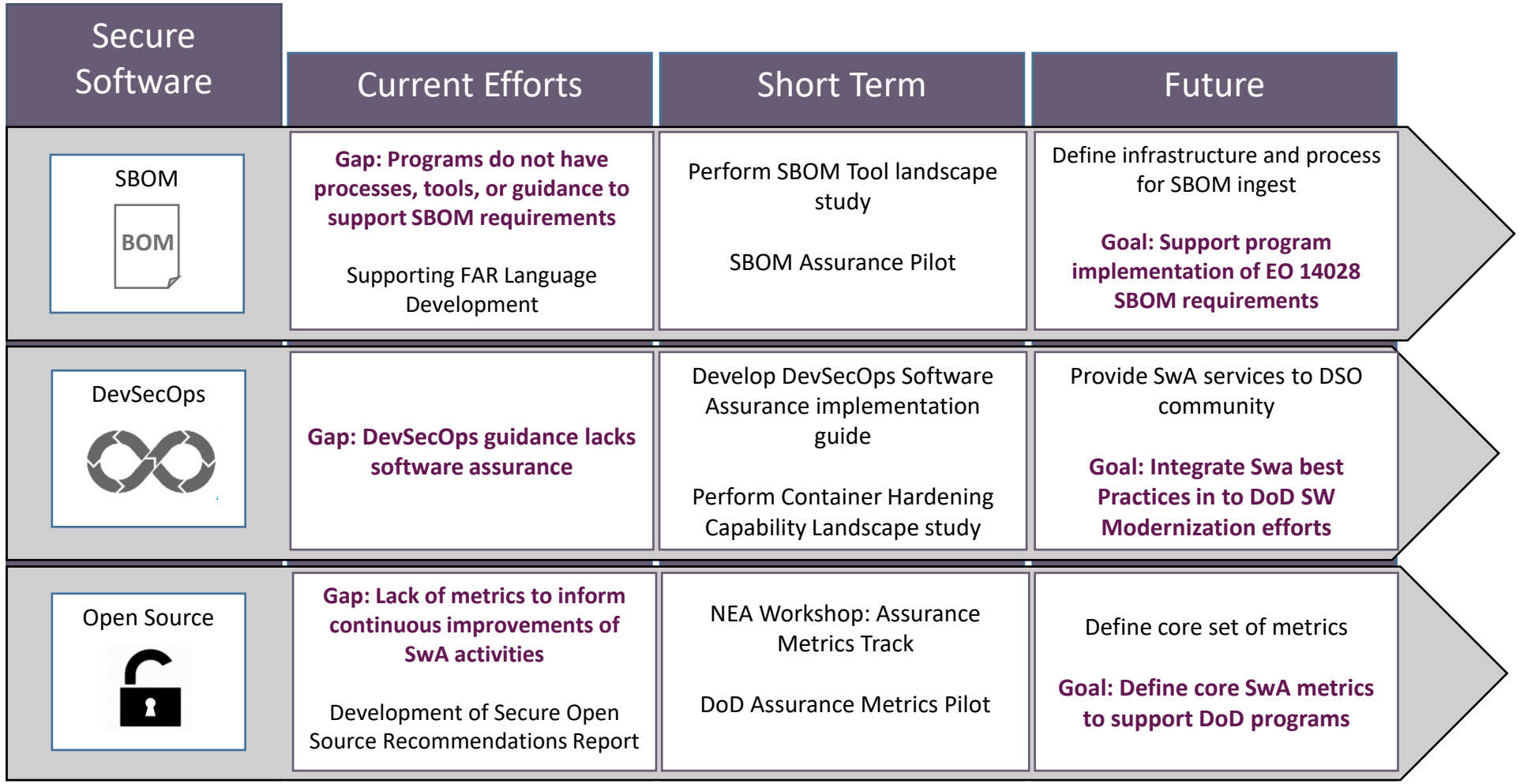
Software Assurance Roadmap
Emerging Technologies

Emerging Technology	Current Efforts	Short Term	Future
Embedded SW 	**Gap: Limited Capability to analyze embedded SW** NSA leading Hardware / Software Assurance Pilot	Identify capability gaps in labs ability to analyze embedded SW Document existing SW analysis and mitigation capabilities	**Goal: Alignment of HW/SW protections for critical microelectronics**
AI & Autonomy 	**Gap: Limited understanding of SwA impacts and protections for AI & autonomy**	Research and whitepapers on SW protections for AI/autonomy SwA for AI / Autonomy Pilot Program	Updates to AI /autonomy whitepapers based on Pilot **Goal: Define SwA best practice for AI and autonomy**
Quantum 	**Gap: Limited understanding of SwA impacts and protections for quantum**	Research and whitepapers on SW protections for quantum	SwA for Quantum Pilot Program **Goal: Define SwA best practice for quantum**
Additional technologies added as prioritized by USD(R&E)			

Software Assurance Roadmap
Maturing Existing Capabilities

Capability Elements	Current Efforts	Short Term	Future
SwA Toolset 	**Gap: Programs do not have access to SwA tools to inform decision making and support analysis**	Perform SwA tool and capability landscape study Define process for SwA tool selection and assessment process	Recommend and implement plan to make identified SwA tools accessible **Goal: Inform program tool selection**
Workforce 	**Gap: Existing SwA expertise is limited and DoD lacks training for future growth**	Develop DAU SwA Credential	Inclusion of SwA best practices in SW and cyber training **Goal: Grow SwA expertise to support program needs**
Metrics 	**Gap: Lack of metrics to inform continuous improvements of SwA activities**	NEA Workshop: Assurance Metrics Track DoD Assurance Metrics Pilot	Define core set of metrics **Goal: Define core SwA metrics to support DoD programs**

Software Assurance Roadmap
Securing Software Development



Software Assurance Roadmap
Advancing the State of Practice

Advancement Opportunities	Current Efforts	Short Term	Future
Partnerships	**Gap: DoD is not fully aligned with UGA on assurance approach and sharing** NEW Workshop & DoD/NNSA SwA CoP	Develop Joint SwA Roadmap with DHS S&T, NSA, & NNSA	**Goal: Align DHS S&T, NSA, & NNSA Assurance efforts to raise assurance posture across departments**
SwA Platform	**Gap: SwA Resources have limited access to expertise and tools required to support programs** Developing AoA for hosting of JFAC infrastructure	Deploy MVP of JFAC Infrastructure to support SwA analysis and tools Prioritize SwA tool offerings and develop timeline	**Goal: Provide comprehensive SwA services to DoD programs**
S&T Innovation	**Gap: DoD lacks awareness of and infrastructure to transition assurance S&T** Coordination with DoD Assurance S&T organizations	Complete Assurance S&T Landscape Study Develop Investment Recommendations Report	Pilot assurance S&T transition **Goal: Make S&T assurance capabilities available early to programs**

Summary

- **Ms. Shyu's memo, "Technology Vision for an Era of Competition," provides clarity, intention, and direction for the future of the Office of the Secretary of Defense for Research and Engineering.**

- **DoD has seen great success with SwA tools, policies, instructions, and guidelines developed and provided to our community. However, the landscape is always changing:**
  - Introduction of new development techniques and tools
  - Discovery of new vulnerabilities
  - Maturing S&T capabilities

- **DoD is looking for input and feedback from NDIA and Industry on how to best address the tools of today and emerging technologies to ensure the U.S. warfighter's ability to counter threats both today and into the future.**

Questions

Steven Grice

Technical Director, Software Assurance

Office of the Under Secretary of Defense
for Research and Engineering

steven.a.grice.civ@mail.mil

Bradley Lanford

SAIC Contractor Support

Office of the Under Secretary of Defense
for Research and Engineering

bradley.p.lanford.ctr@mail.mil