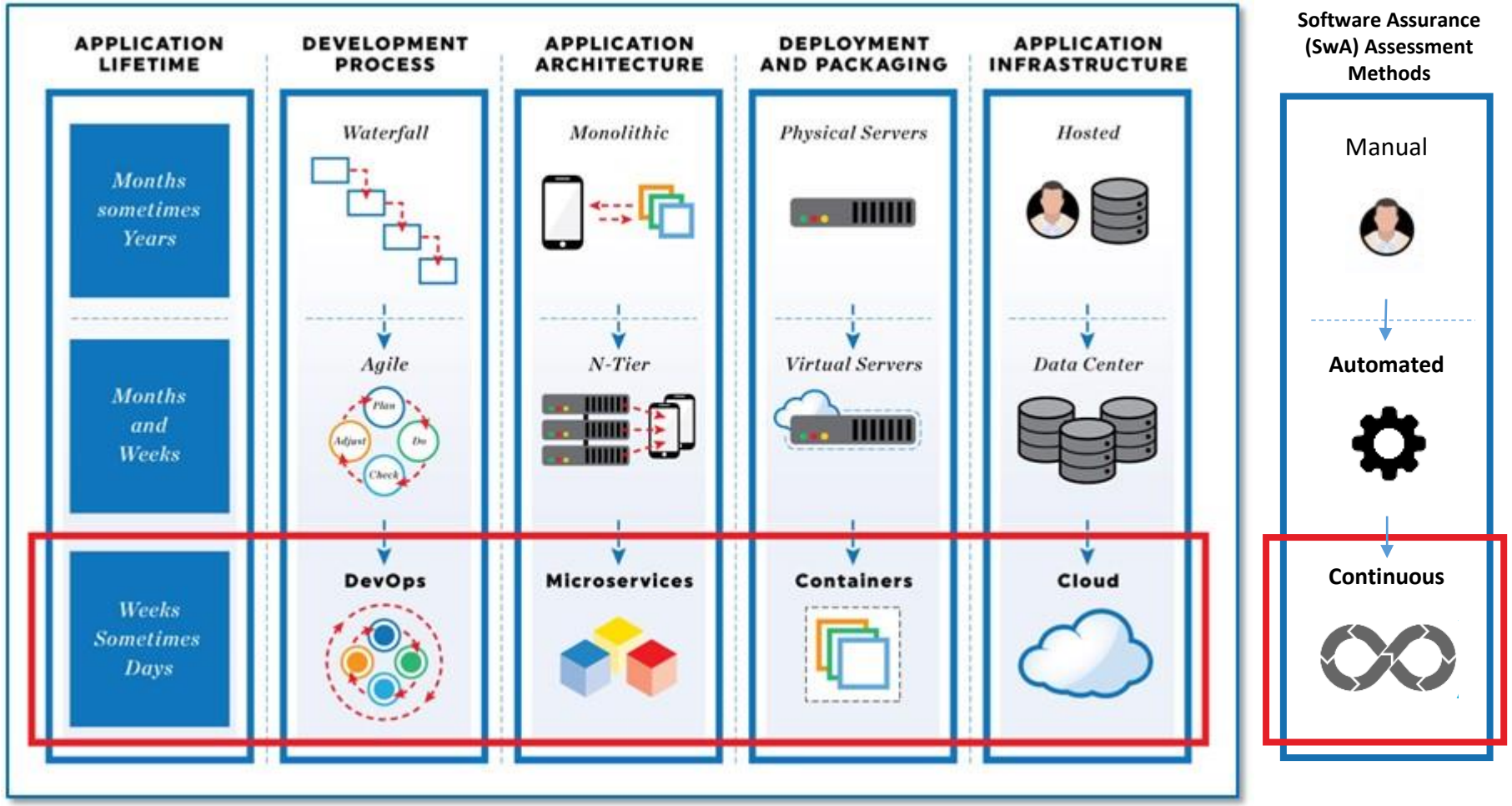
Joint Federated Assurance Center Development, Security, and Operations (DevSecOps) Strategy

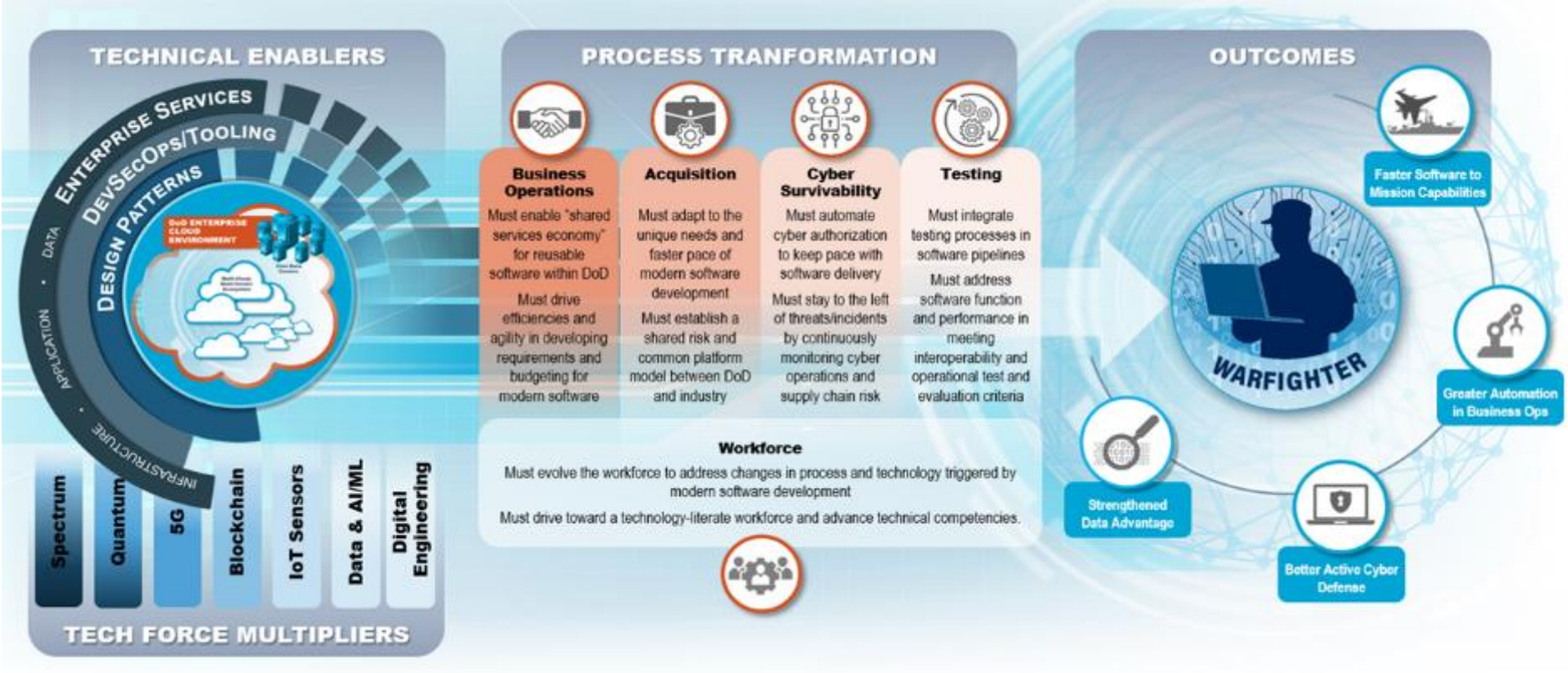
Bradley Lanford
Software Assurance Lead, Contractor Support
Office of the Under Secretary of Defense for Research and Engineering

National Defense Industrial Association Systems & Mission Engineering Conference
December 6-8, 2021

Software Evolution



Software Modernization Strategy



Goal 1: Accelerate the DoD Enterprise Cloud Environment

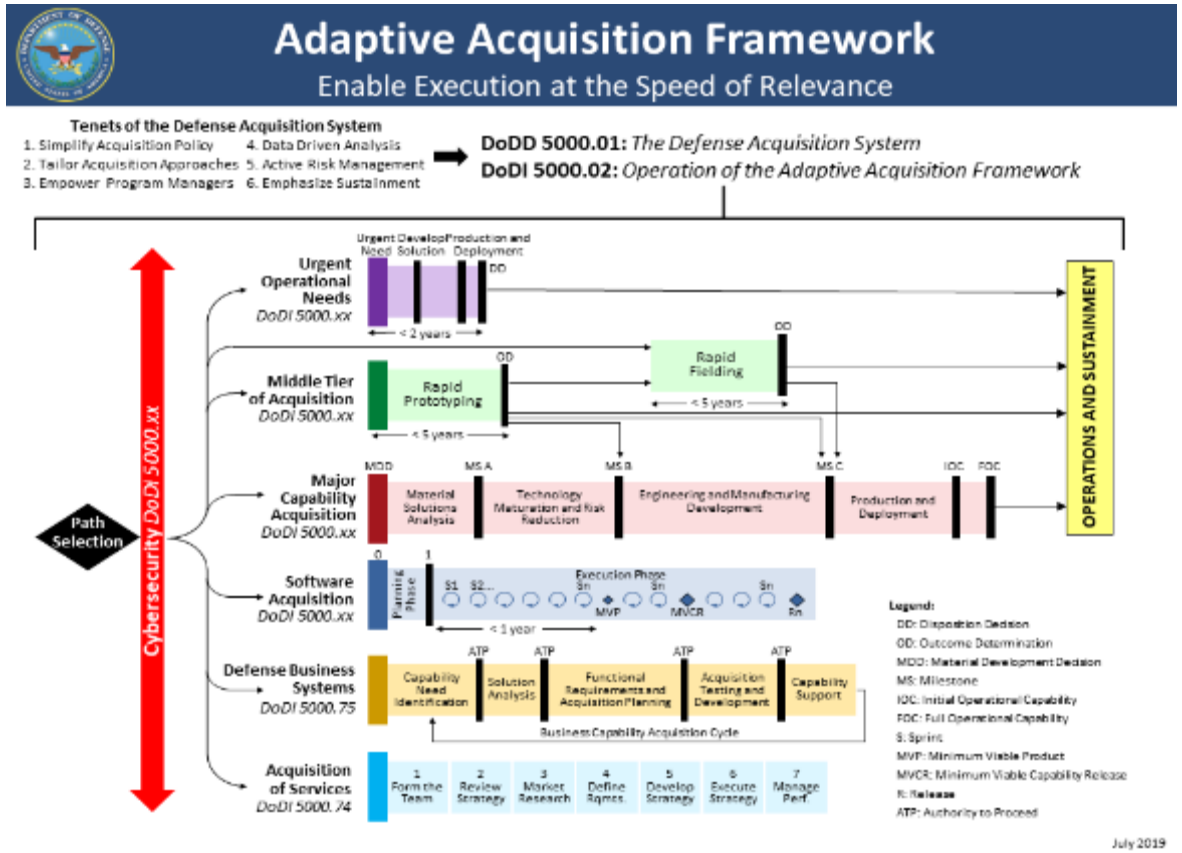
Goal 2: Establish Department-wide Software Factory Ecosystem

Goal 3: Transform Processes to Enable Resilience and Speed

SwA Impacts of the Adaptive Acquisition Framework (AAF)

Technology Modernization Priorities

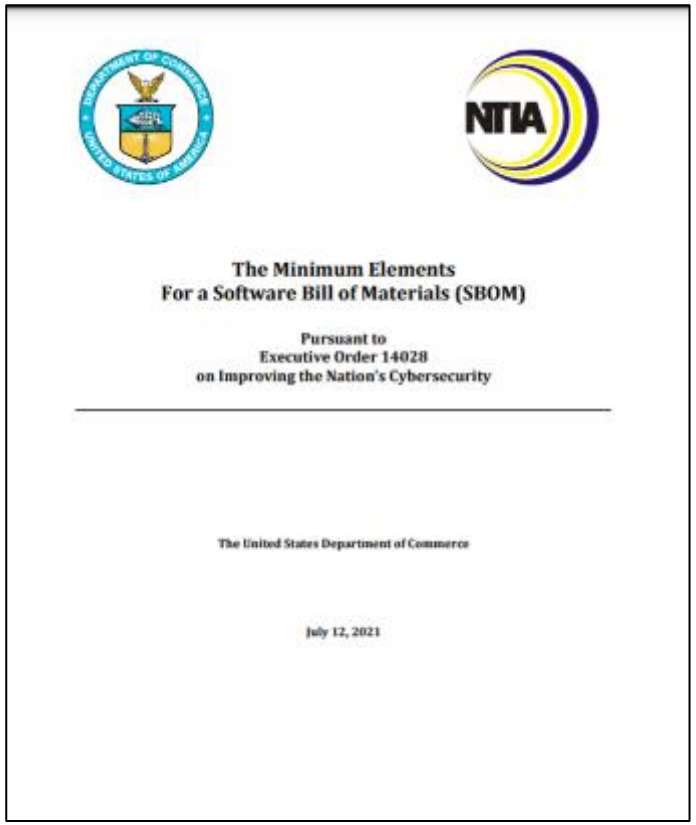
- 5G Network Technology
- Autonomy
- Biotechnology
- Cyber
- Directed Energy
- Fully Networked Command, Control, and Communications
- Hypersonics
- Machine Learning / Artificial Intelligence
- Microelectronics
- Quantum Science
- Space



S&T Protection | **Program Protection**

Technology Area Protection Plans for DoD Modernization Priorities

Executive Order (EO) 14028



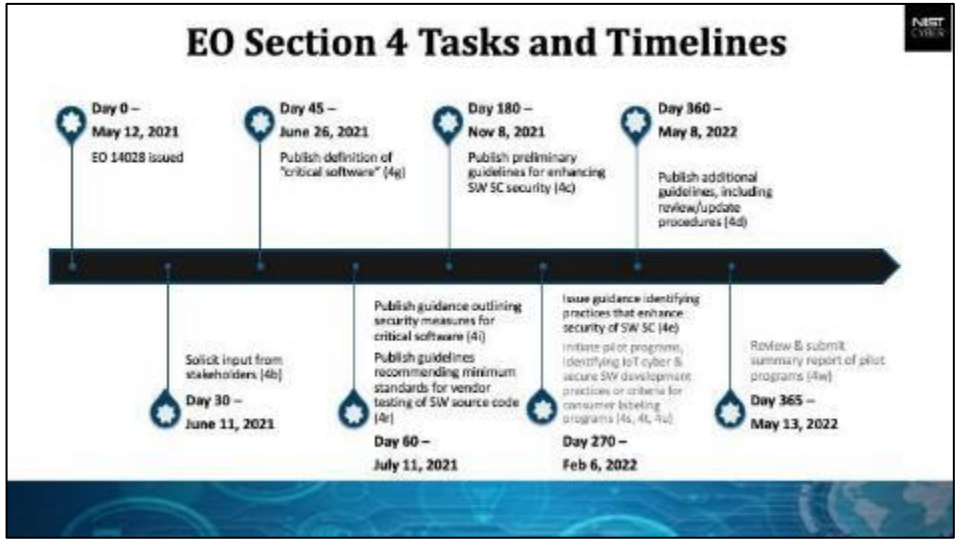
The Minimum Elements
For a Software Bill of Materials (SBOM)

Pursuant to
Executive Order 14028
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

EO 14028, Section 4(n) - FAR/Contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections 4(g) through 4(k).



SwA in the AAF

SwA

Statutory for Covered Systems (Major Systems, NSS, Mission Assurance Category 1 Systems). 10 USC 2224, Note Pub L 112-239, as amended, *Improvement in Assurance of Computer Software Procured by the Department of Defense*. Department of Defense Instruction (DoDI) 5000.83

- Mandatory for Covered Systems
- Mandatory for Covered Systems
- Mandatory
- Mandatory for Covered Systems
- Recommend Best Practice
- N/A

SwA in Urgent Capability Acquisition

- **The purpose of the Urgent Capability Acquisition pathway is to field capabilities to fulfill urgent operational needs or reactions as quickly as possible and in less than two years.**

- **The program protection analyses are streamlined to execute in UON short timeframes (e. g. hours or days) to ensure a secure fielded system.**

- **Software supply chain protections are emphasized to promote the use of readily available software.**

- **Software Protection Considerations:**
  - Employing secure software design, architecture, standards, analysis tools, and tests
  - Identifying and documenting vulnerabilities with associated risks
  - Identifying and incorporating protection measures to bring risks within acceptable range
  - Software Bill of Materials

SwA in Middle Tier Acquisition

- **The Middle Tier of Acquisition (MTA) pathway includes Rapid Prototyping and Rapid Fielding programs. The level of maturity enables MTA rapid prototyping within five years and rapid fielding initiation within six months (unless waived by the Defense Acquisition Executive) and completion of rapid fielding within five years.**

- **Rapid Prototyping SwA Considerations:**
  - SwA methods and practices should be considered early to avoid delays in fielding
  - Each iteration of prototyping should be analyzed for vulnerabilities and security risks
  - Plans for software transition should be considered

- **Rapid Fielding SwA Considerations:**
  - Employing secure software design, architecture, standards, analysis tools and tests
  - Identifying and documenting vulnerabilities with associated risks
  - Identifying and incorporating protection measures to bring risks within acceptable range
  - Software Bill of Materials

SwA in the Software Acquisition Pathway

- **The Software Acquisition Pathway is used to facilitate rapid and iterative delivery of software capability to the user. The Pathway specifies that cybersecurity and program protection are continuously addressed from program inception through capability delivery.**
  - Program protection requirements should be identified in the capability needs statement
  - Use of enterprise services allows programs to inherit protections implemented by the infrastructure, platform, or software service providers
  - Assurance methods and practices should be automated to the greatest extent possible

- **Software Acquisition SwA Considerations:**
  - Employing and automating, to the maximum extent practicable, secure design, architecture, standards, analysis tools, and tests
  - Generating or using shared artifacts to identify vulnerabilities with associated risks
  - Identifying artifacts to inform approval of program protection actions and fielding with any residual risk
  - Inherited protections through the use of enterprise services and the impact to the overall assurance of the system

SwA in Defense Business Systems

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.

- Department of Defense Instruction (DoDI) 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” program protection policy does not apply to this pathway, but program protection recommended practice is to assess the COTS products used for vulnerabilities.

- Many DBS programs use enterprise software packages that need to be customized. Secure software standards need to be established for the customizations along with vulnerability testing to identify and mitigate vulnerabilities.

- Protection of the interfaces between COTS products, and customizations as well as external interfaces will reduce the exposure of vulnerabilities.

Technology Transition Opportunities

Sources for Proposed S&T Maturation

Software Engineering Institute
- $20M in R&E funding
- 6.2 – 6.3 efforts

D, Cyber Technology
- ~$20M in directed funding
- 6.2 – 6.3 efforts

External Sources
- Service Recommendations
- DARPA
- Other FFRDCs

JFAC Technical Working Group Prioritization and Roadmap

Target Customers

DoD Programs
- Army
- Navy
- USAF

JFAC SwA Service Providers
- Services
- NSA
- Other

JFAC Partners
- NNSA
- PD Micro
- Industry

DDRE(R&T) Software Maturation
- Opportunity to expand beyond Assurance Solutions leveraging as built ecosystem
- Identified as #1 enabler of SW technology transition

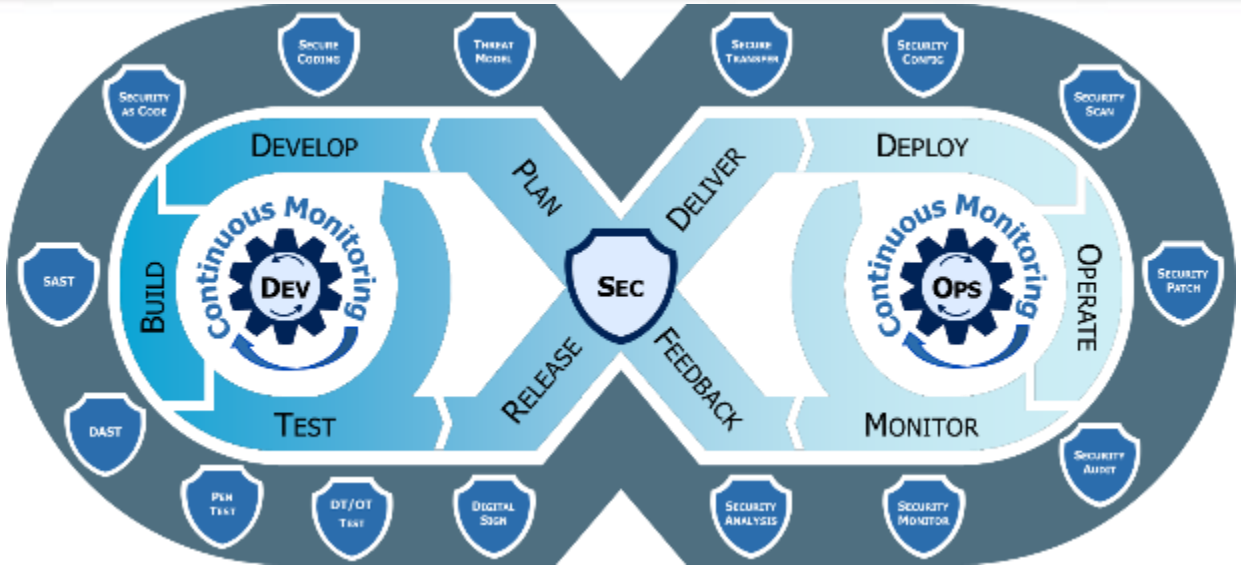
JFAC Ecosystem

- Centralized hosting environment
- IaC for reuse to speed ATO and standup
- Common set of best practices
- Containerization to greatest extent
- Existing customer base

Continuous Engagement
- Informs S&T needs
- Engages industry
- Enhances SwA toolbox
- Supports government decisions

Mature &Transition
- Identifies transition partners
- Builds artifact repository

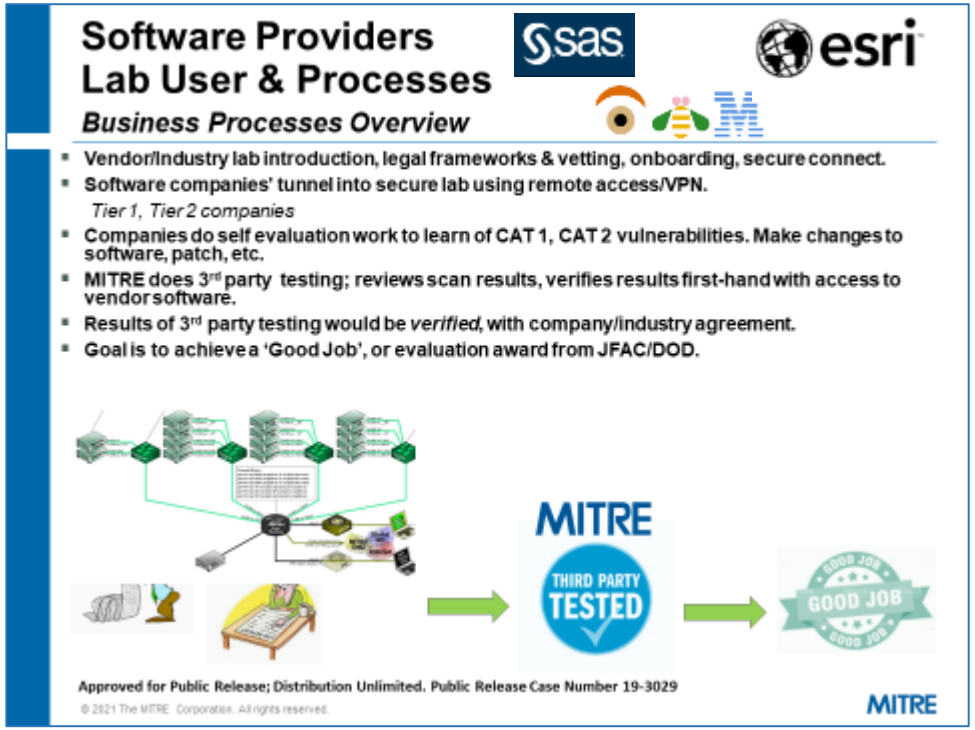
Evaluating SwA in DevSecOps

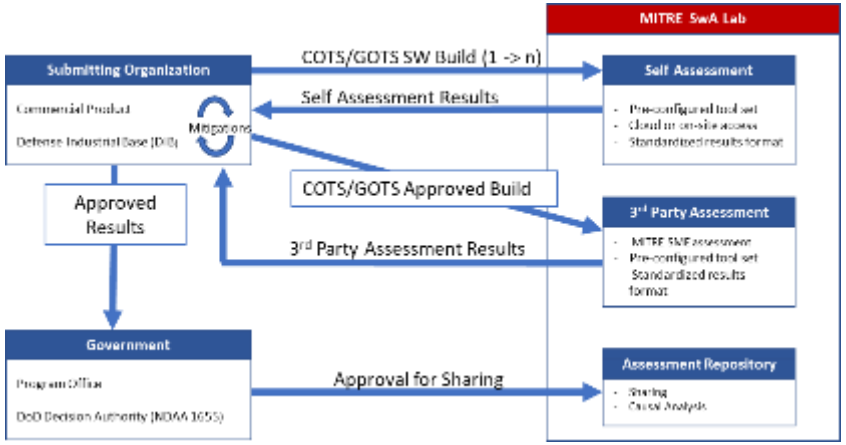


Lifecycle Assurance Practices	Critical Component Assurance	Domain Specific Assurance Impacts	Science and Technology Assurance Impacts
Culture (Barriers and Silos) Development Tools Configuration Management Container Hardening Infrastructure/Security as Code Secure Coding Practices CI/CD Tooling SAST/DAST Incident Management Red Teams Continuous Monitoring	Requirements Management Repositories Integrated Dev Environments Agile Management Build/Integration Container Security Orchestration Cloud Security Reporting and Analytics Test Automation	Web Applications C4ISR Embedded DBS Autonomous Systems	OSS Repositories Tool Automation Digital Engineering SBOM Hardware in the Loop AI/ML

Third Party Acquisition and Assurance Lab

- **MITRE Acquisition and Assurance Lab provides a security testing and certification technology that achieves risk mitigation for both industry and the government**
  - Industry receives secure access to an assessment environment and tools to streamline government procurement decisions
  - DoD Services are able to validate assurance practices without access to proprietary processes or source code





Fiscal Year 2021 Accomplishments

- Executed proof of concept for lab environment and external access
- Completed first third party industry assessment and developed report
- Engaged Kessel Run to determine environment, tools and threshold opportunities
- Identified and began integration of commercial tools to enhance lab capabilities

Questions