Joint Federated Assurance Center Software Assurance Strategy

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

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

Introduction

- **The Joint Federated Assurance Center (JFAC) was established to ensure the security of software and hardware developed, acquired, maintained, and used by the Department of Defense (DoD) through the federation of existing DoD software and hardware assurance resources, expertise, and capabilities.**

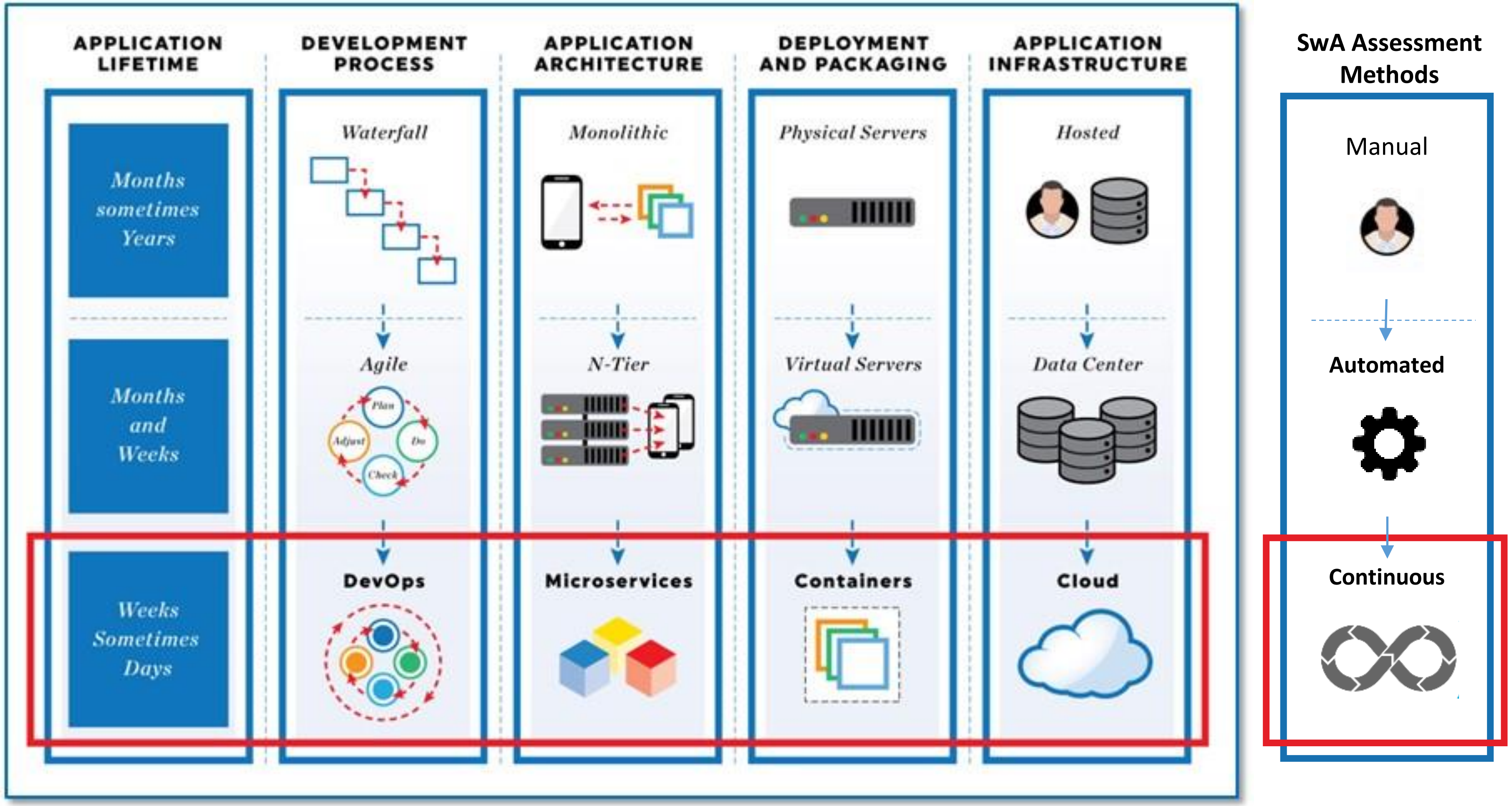
- **Federal and Department initiatives are revolutionizing application of software assurance tools, practices, and techniques:**
  - Development, Security, and Operations (DevSecOps)
  - Zero Trust Architecture
  - DoD Adaptive Acquisition Framework Software Acquisition Pathway
  - Executive Order 14028 – Improving the Nation’s Cybersecurity

- **The JFAC Modernization Strategy for Software Assurance was developed to support the software assurance initiatives:**
  - Focus on opportunities to overcome resource limitations to provide capabilities and expertise directly to DoD programs
  - Leverage existing DoD software initiatives to modernize JFAC infrastructure and capabilities
  - Transition culture away from the development of capabilities to the federation and maturation of existing tools and resources

JFAC Historical Overview

Growth of JFAC		State of Software Assurance (SwA)
National Defense Authorization Act (NDAA) Section 933 required the establishment of a baseline for SwA in policy	FY 2013	Estimated 27% of known vulnerabilities remediated by government, Veracode ‘13-15
NDAA Section 937 established JFAC as a federation of capabilities	FY 2014	Government spending on Information Technology (IT) defenses vs. SwA analysis 23:1, Gartner ‘14
JFAC Charter signed by Deputy Secretary of Defense	Q2 2015	84% of breaches exploit vulnerabilities in the application, Forbes ‘15
JFAC Concept of Operations (CONOPS) approved establishing JFAC Coordination Center	Q3 2015	Common Vulnerability Scoring System (CVSS) Version 3 published for SW vulnerability evaluation
JFAC Portal (Army.mil) and Coordination Center (SEI) capability established	FY 2016	NDAA FY16 Section 1647 requires the evaluation of cyber vulnerabilities for all weapons systems
Consolidation of Portal and Coordination Center Hosting (NSERC)	FY 2017	NDAA FY17 Section 1650 requires the evaluation of cyber vulnerabilities for critical infrastructure
Increase in Coordination Center support for tool metrics, AKB, SIPR/JWICS portal	FY 2018	DSB identifies opportunities to address SW vulnerabilities with iterative development and tool chains

Software Evolution



APPLICATION LIFETIME	DEVELOPMENT PROCESS	APPLICATION ARCHITECTURE	DEPLOYMENT AND PACKAGING	APPLICATION INFRASTRUCTURE	SwA Assessment Methods
Months sometimes Years	*Waterfall*	*Monolithic*	*Physical Servers*	*Hosted*	Manual
Months and Weeks	*Agile*	*N-Tier*	*Virtual Servers*	*Data Center*	**Automated**
Weeks Sometimes Days	**DevOps**	**Microservices**	**Containers**	**Cloud**	**Continuous**

SwA Modernization Roadmap

FY 2019 - FY 2021

Capabilities that Deliver Tangible Value across DoD

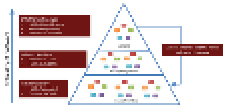
#1 Guidance and Training

#3 Software Assurance Tools/Licenses

#2 Knowledge Base of Tools, use, and Components

#4 JFAC Support Services

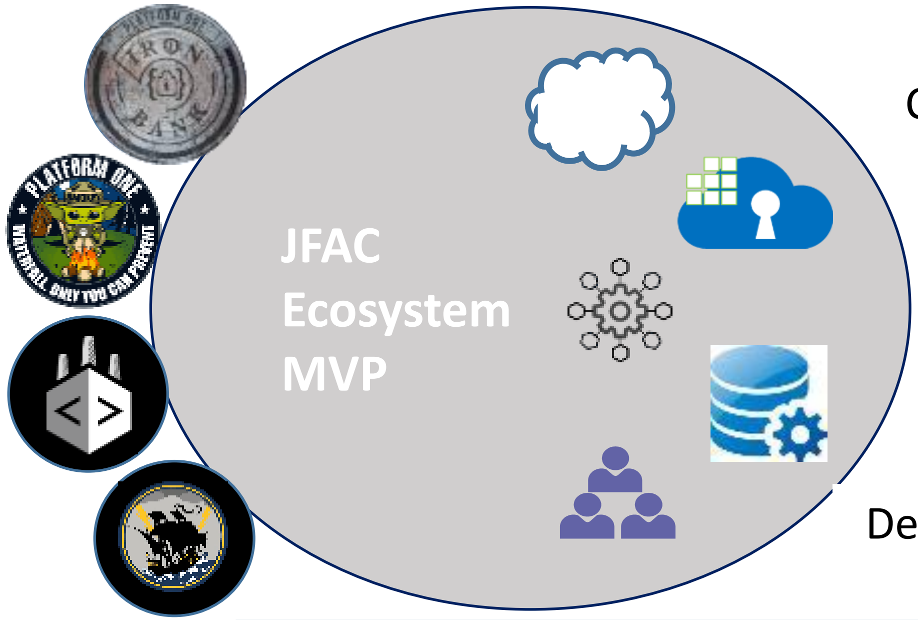
- JFAC Portal
- Assurance Knowledge Base
- Licenses Distribution

FY 2021 Efforts Pilot initial capabilities and performance measures	FY 2022 Develop Infrastructure	FY 2023 Establish Capabilities	FY 2024 Capabilities Deploy to Service Providers and Programs
MITRE *Technology & Innovation Roundtable*™ Assurance Lab Pilot	CLOUD ONE amazon webservices Microsoft Azure Identify cloud provider and core services		• Platform as a Service (PaaS) • Integrated/Swappable Tools • Risk Categorization Engine
Red Hat Enterprise Linux & kubernetes			• Software as a Service (SaaS) • Automated SwA Analysis • Secure Artifact Repository
DoD/NNSA Malware Discovery Exercise (MDX) 			• Software as a Service (SaaS) • Packaged tool solution • Secure, SBOM, & POA&M
JFAC Tools & License Distribution	Streamline Infrastructure	Modernization	• Streamlined information to programs • Modernized Approach (EO 14028) • Inform procurement (NDAA 1655)
JFAC Technical Working Group	• Development S&T Roadmap • Identification Hard Problems • Prioritization SwA Gaps and Performers		Iterate

Modernization Strategy for Software Assurance

Goal: Assurance as a Service

Create an environment, leveraging existing Software Factories, to provide tools and capabilities available to SwA Service providers and programs.



Cloud Native Assessment Environment

Assured Pipeline and Repository

Technology Maturation and Transition

Software Assurance Toolkit and License

Decentralized Assessments/Automation of Alerts

Key enablers to drive maturity
Standardization of processes to enable automation
Science & Technology investment to mature assurance capabilities
Education of service providers to transition culture

Software Assurance as a Service

- **Transition away from the federation of self-hosted assurance capabilities towards existing cloud native assurance services.**

- **Minimum Viable Product ecosystem will include:**
  - Platform-as-a-Service environment allowing remote access to automated assurance pipelines
  - Software-as-a-Service assurance capabilities available to all DoD programs
  - DoD accessible repository for access to assured tools, components, and S&T
  - Toolkit for access to assurance resources in offline environments

- **Roadmap Overview:**
  - FY21: JFAC Modernization Strategy for Software Assurance developed
    - Incorporates lessons learned and adoption of new practices
  - FY22: Streamline existing JFAC infrastructure; identify cloud capabilities to support transition
  - FY23-24: Create a collaborative ecosystem to promote and make available tools and capabilities for program use
    - Leverages JFAC SwA Technical Working Group recommendations, maturation of S&T, and federation of existing capabilities into the cloud native environment

Advancement of Software Assurance

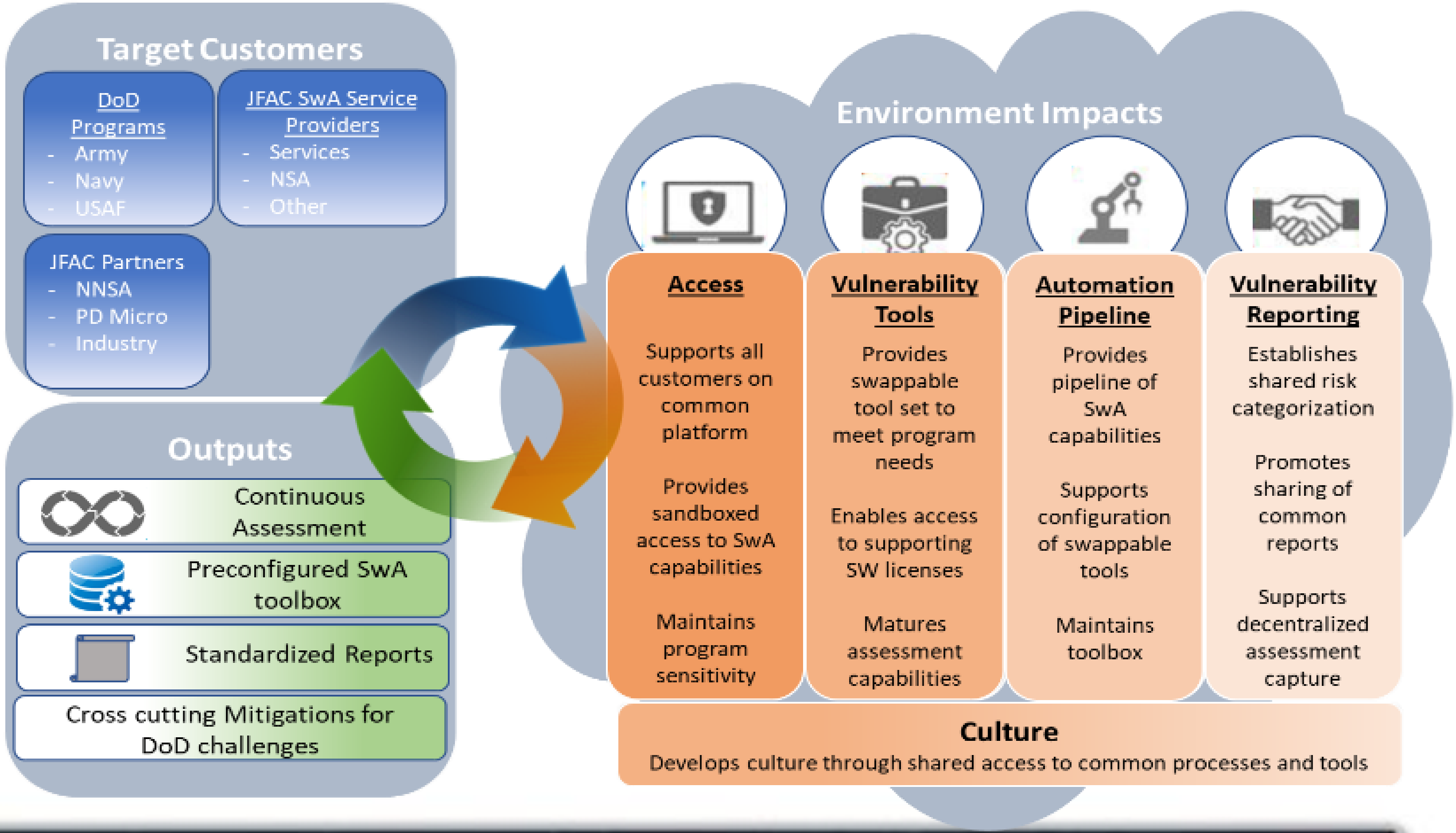
	2017 (IOC)	2020 (FOC)	2024 (AaS)
Federation of SwA Capabilities	Identification of disparate capabilities throughout DoD	Federation of capabilities and sharing of best practices	Sharing of capabilities and data through centralized infrastructure
	Automated testing is estimated to grow from $12.6 billion in 2019 to $28.8 billion by 2024		
Program Support	Individual support based on local resources and capabilities	Centralized resource to access support organizations with limited bandwidth	Maximized support through centralized and automated resources
	By 2025 organizations will speed up remediation of SAST vulnerabilities by 30% through automation		
Software Assurance Tools	Budget restricted tool buy to support limited programs	Small increase in license availability with yearly buys and distribution	Continued tool buys supplemented by OSS and GOTs shared capabilities as a service
	By 2024 more than 45% of IT infrastructure and infrastructure software will move to cloud services		

Capability will enhance federation of software assurance capabilities and distribution of software assurance tools to maximize program support

JFAC Environment Capabilities

Provide a centralized resource for DoD programs that offers:

- Consolidation of effective assurance capabilities
- Common risk categorization and reporting
- Increased assurance rigor through automation



Target Customers

DoD Programs
- Army
- Navy
- USAF

JFAC SwA Service Providers
- Services
- NSA
- Other

JFAC Partners
- NNSA
- PD Micro
- Industry

Outputs

- Continuous Assessment
- Preconfigured SwA toolbox
- Standardized Reports
- Cross cutting Mitigations for DoD challenges

Environment Impacts

Access

Supports all customers on common platform

Provides sandboxed access to SwA capabilities

Maintains program sensitivity

Vulnerability Tools

Provides swappable tool set to meet program needs

Enables access to supporting SW licenses

Matures assessment capabilities

Automation Pipeline

Provides pipeline of SwA capabilities

Supports configuration of swappable tools

Maintains toolbox

Vulnerability Reporting

Establishes shared risk categorization

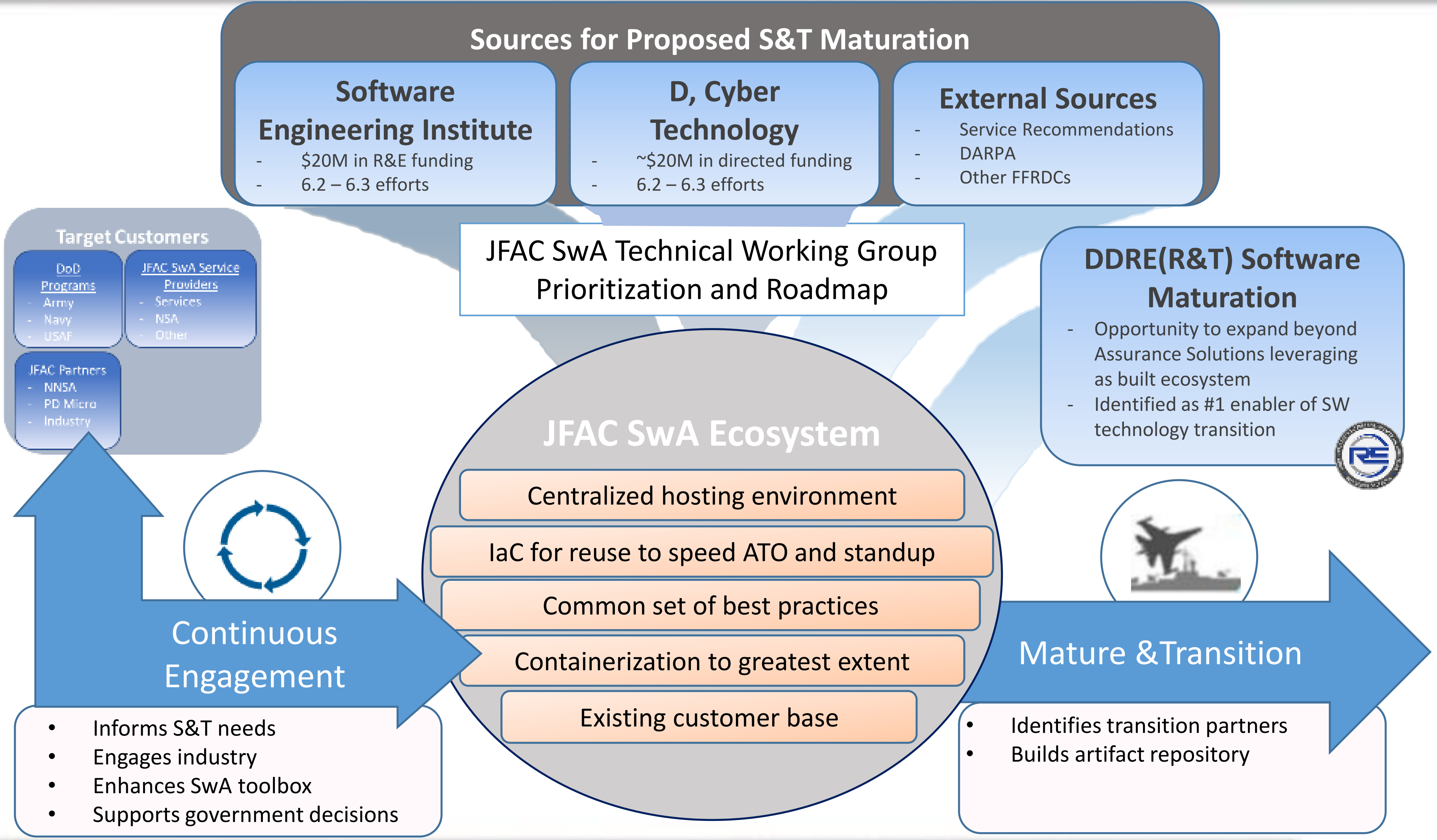
Promotes sharing of common reports

Supports decentralized assessment capture

Culture

Develops culture through shared access to common processes and tools

Software Assurance 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 SwA 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

JFAC SwA Ecosystem

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

DDRE(R&T) Software Maturation

- Opportunity to expand beyond Assurance Solutions leveraging as built ecosystem
- Identified as #1 enabler of SW technology transition

Continuous Engagement

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

Mature &Transition

- Identifies transition partners
- Builds artifact repository

JFAC SwA Technical Working Group
Way Ahead

Gap Analysis Prioritization

Review and update of 2017 capability gap analysis

- Prioritize of gaps based on risk and value
- Inform JFAC Strategy implementation

S&T Roadmap

Develop SwA Science and Technology Roadmap

- Lead identification of efforts for proposed investment
- Recommend performers and steps for maturation

Hard Problem Analysis

Make available mitigations directly impacting program

- Identify future SwA gaps and mitigations
- Support service providers and programs through federation of knowledge

JFAC Infrastructure Transition

Software Licensing

Program Support

Body of Knowledge

Procurement Support

Streamline infrastructure to support critical needs (MVP)

COTS Licenses Distribution

Support Services

Document Repository

Assessment Capture

Modernization to operate in cloud native environment

- SaaS containerized tool offerings
- BOAs for licensing
- Utilization of GOTS/FOSS tools

- Software Service Provider use of PaaS solutions
- Access to SaaS toolkit

- Access to enterprise cloud services
- Link to existing services to strengthen BoK

- Partner with JFAC HwA
- Automation of alerts and assessment findings

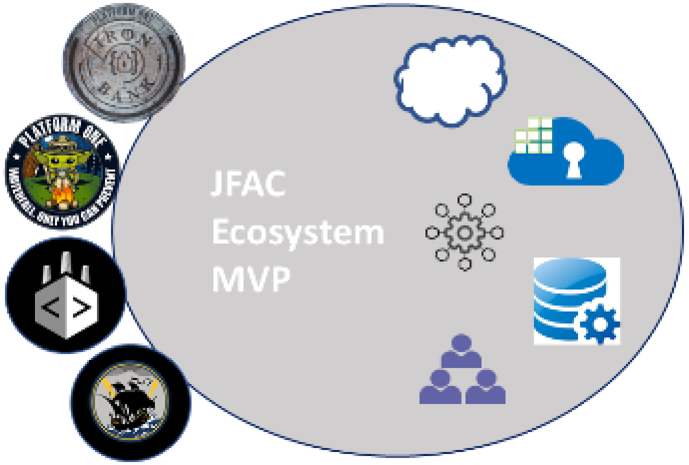
Partnerships

- **DoD DevSecOps Initiative**
  - Coordination of Assurance Platform with DoD SW factories to promote adoption and support DSO efforts
  - Alignment of JFAC Enterprise Software Licenses with platform centralized contract vehicle
  - Recognition for JFAC as leader in technical assessment capabilities through support to DSO initiatives
- **Principle Deputy for Microelectronics Office**
  - Centralized JFAC infrastructure to support HwA and SwA cloud service offerings
  - Single source of assessment information with distributed capabilities and tracking
- **National Nuclear Security Administration (NNSA)**
  - Utilization of Operational Technology and Software Engineering Lifecycle Assurance Guide
  - Promotion of NNSA capabilities as SaaS offerings
  - Coordination with NNSA labs and plants through PaaS and SaaS offerings
- **Military Services and DoD Agencies**
  - Maturation of COTS solutions and distribution to DoD organizations through cloud service offerings
  - Support for existing service providers with PaaS and SaaS capabilities
  - Investment in S&T and identification of partners to advance SwA capabilities

FY22 Planning

Goal: Enhance federation of SwA capabilities and distribution of SwA tools to maximize program support

- **Standardization and advancement of existing JFAC capabilities**
  - Kubernetes / Redhat Phase 3
  - Acquisition and assurance lab pilot
  - Risk categorization
- **Identification of software and platform service offerings**
  - Software factory capabilities
  - Centralized artifact repositories (IronBank)
  - Container hardening processes
- **Recommendations for maturation and transition of S&T capabilities**
  - Investment of 6.4 funding to mature 6.2 / 6.3 efforts
  - Advancement of assurance tools and capabilities
  - Integration of assurance into cybersecurity S&T
- **Respond to Congressional and Executive Orders**
  - Recommendations for JFAC SwA procurement
  - Assessment and identification of mitigations supporting FY19 NDAA Section 1655
  - Testing and SBOM standards supporting Executive Order 14028



Performance Metrics

- Collaborate with partners to develop metrics that measure outcomes
  - Promote successes
  - Enable change

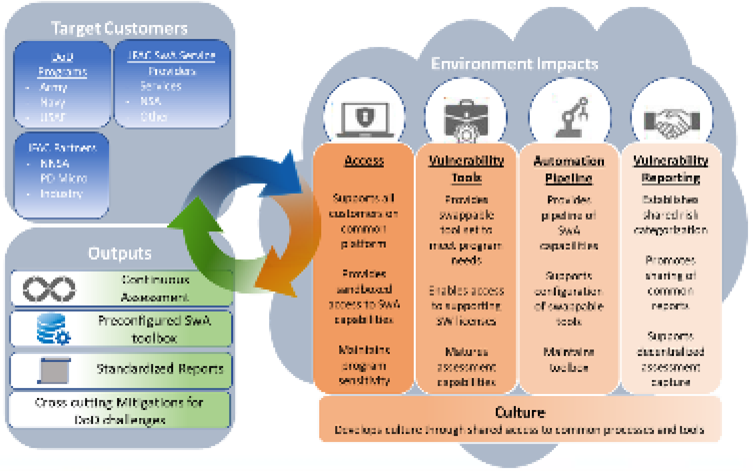
Efforts	Proposed Metrics
Cloud Native Assessment Environment	# of utilized JFAC PaaS offerings, # of downloads, # of capabilities made available through cloud environment
Assured Pipeline and Repository	# and involvement of partner organizations supporting JFAC efforts, # of products assessed, % adoption of JFAC services across DoD
Software Assurance Toolkit	# of programs/service providers utilizing SaaS offerings, # of tools available in SwA toolkit
Tools and License Distribution	# of assessments identified, # of federated organizations, # of licenses distributed, # of programs supported
Technical Working Group	# SwA gaps identified/resolved, # of technology transitions, completion of S&T Roadmap

Summary

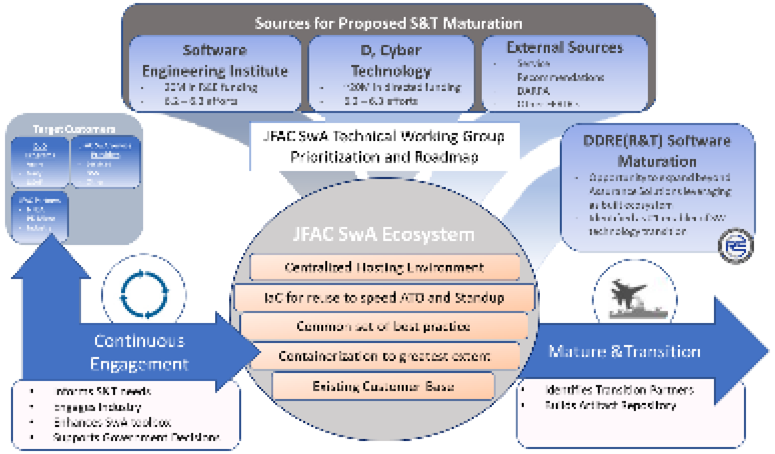
- **DoD transition to a DevSecOps ecosystem, adoption of modern architecture patterns, and adherence to DevSecOps best practices drives the need for modernization of JFAC infrastructure and program support.**

- **JFAC FY 2022-2024 SwA Strategy provides means to proactively increase mitigation of software vulnerabilities. Strategy includes:**
  - Instantiation of JFAC ecosystems to support platform and SwA services
  - Emphasis on JFAC SwA Technical Working Group expertise to guide project decisions
  - Renewed focus on performance metrics to support Department growth

- **OUSD(R&E) JFAC ecosystem facilitates federated DoD software and assurance capabilities:**
  - Provides access to assessment capabilities for all DoD programs
  - Creates a platform for maturation and transition of S&T efforts



Target Customers
DoD Programs
Army
Navy
USAF
JFAC SwA Service Providers
Services
NSA
Other
JFAC Partners
NNSA
PD Micro
Industry
Outputs
Continuous Assessment
Preconfigured SwA toolbox
Standardized Reports
Cross cutting Mitigations for DoD challenges
Environment Impacts
Access
Supports all customers on common platform
Provides sandboxed access to SwA capabilities
Maintains program sensitivity
Vulnerability Tools
Provides swappable tool set to meet program needs
Enables access to supporting SW licenses
Matures assessment capabilities
Automation Pipeline
Provides pipeline of SwA capabilities
Supports configuration of swappable tools
Maintains toolbox
Vulnerability Reporting
Establishes shared risk categorization
Promotes sharing of common reports
Supports decentralized assessment capture
Culture
Develops culture through shared access to common processes and tools



Sources for Proposed S&T Maturation
Software Engineering Institute
$2M 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 entities
Target Customers
JFAC SwA Technical Working Group Prioritization and Roadmap
DDRE(R&T) Software Maturation
Opportunity to expand beyond Assurance Solutions leveraging a built ecosystem
Identifies S&T candidates for SW technology transition
JFAC SwA Ecosystem
Centralized Hosting Environment
IaC for reuse to speed ATO and Standup
Common set of best practice
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

Questions

Backup

References

Automated testing growth:
https://www.marketsandmarkets.com/Market-Reports/automation-testing-market-113583451.html#:~:text=What%20is%20the%20market%20size,18.0%25%20during%20the%20forecast%20period

Increase in SaaS :
https://www.forbes.com/sites/forbescommunicationscouncil/2021/02/24/saas-trends-to-watch-in-2021/?sh=18cb87565385

Application Security Testing Automation:
https://www.gartner.com/doc/reprints?id=1-1YADS6J8&ct=200206&st=sb

Transition to the Cloud:
https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/