DoD Enterprise DevSecOps Community of Practice

March 11, 2021

Agenda

- Opening Remarks
- Digital Engineering as a Service
  - Air Force
- Platform One Update
  - Air Force
- Overview of PEO Roadshow for Software Modernization
  - OUSD(A&S)
- Closing Remarks

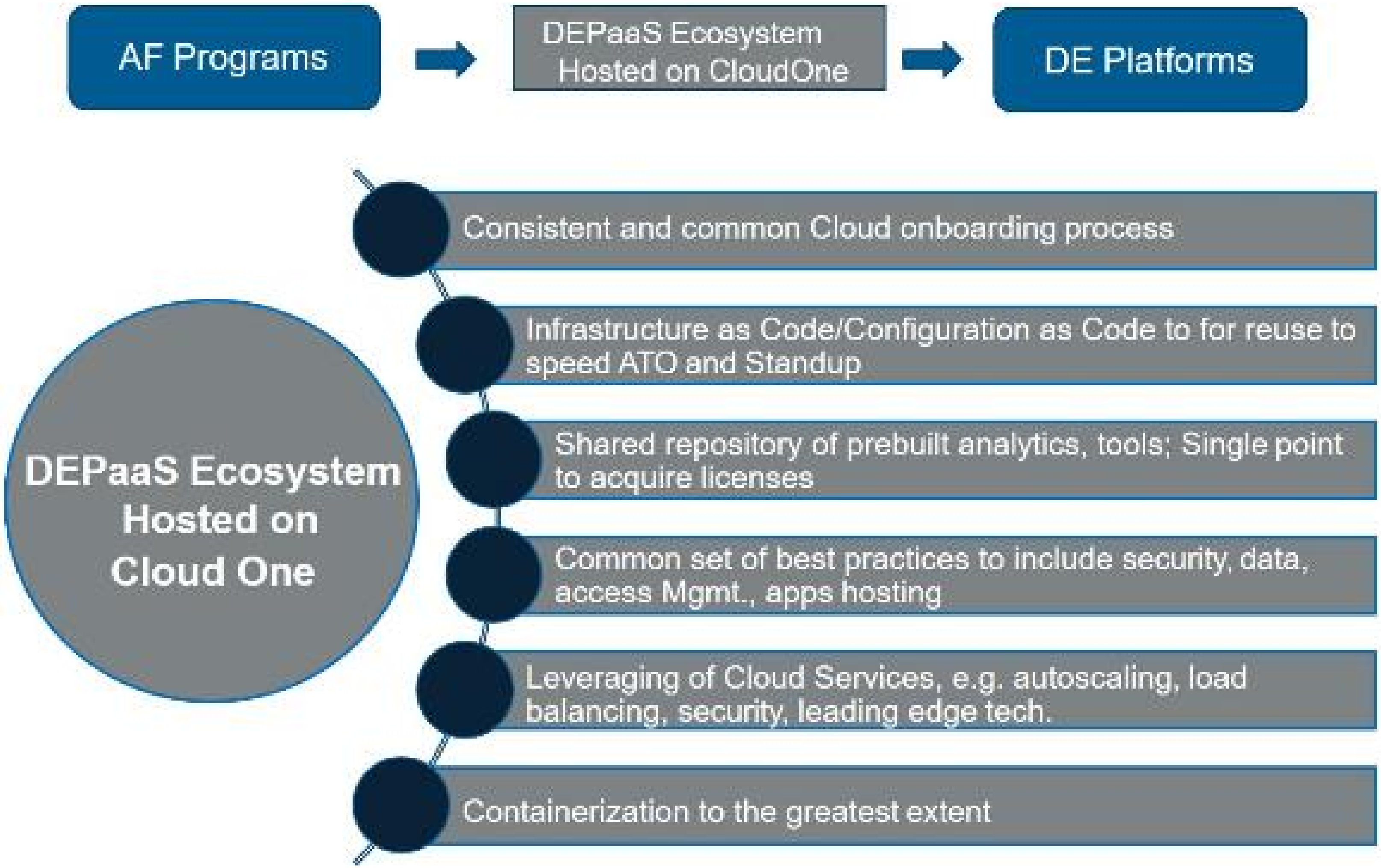
Opening Remarks

PEO C3I&N
Digital Engineering Platform

Brian Kropa
Chief Engineer
AFLCMC/HNI
Enterprise IT
& Cyber Infrastructure
11 MAR 2021

Digital Engineering Platform MVP

Cross-Cutting effort between AFLCMC/XA, ABMS, USSF SMC, GBSD, MITRE and HN



AF Programs → DEPaaS Ecosystem Hosted on CloudOne → DE Platforms

DEPaaS Ecosystem Hosted on Cloud One

- Consistent and common Cloud onboarding process
- Infrastructure as Code/Configuration as Code to for reuse to speed ATO and Standup
- Shared repository of prebuilt analytics, tools; Single point to acquire licenses
- Common set of best practices to include security, data, access Mgmt., apps hosting
- Leveraging of Cloud Services, e.g. autoscaling, load balancing, security, leading edge tech.
- Containerization to the greatest extent

Digital Engineering Platform MVP

Tools

Cameo

- Architecture Management
- Model Based System Engineering

Teamwork Cloud Server

- Cameo Model Repository

DOORS

- Requirements Management
- Concurrent Users

AFSIM

- Modeling and Simulation (M&S) of Operational Scenarios

Collaboration Tools

- P1 – Confluence/Jira*

Onboarding / New Requirements

- Work with Customer on digital requirements
- Pipeline for agile development and incremental updates
- DE Cyber Reference Architecture

Infrastructure

- VDI for DE Tool Utilization*
- CAC enabled SSO
- Migrating to leverage CNAP

Account Provisioning

- Customer will register users
- C1/SAIC will create the accounts inside of the DE environment

Sustainment of Tools and Infrastructure

- Patching, Upgrades, and Maintaining Cybersecurity Posture
- Software License Management (e.g. renewals)

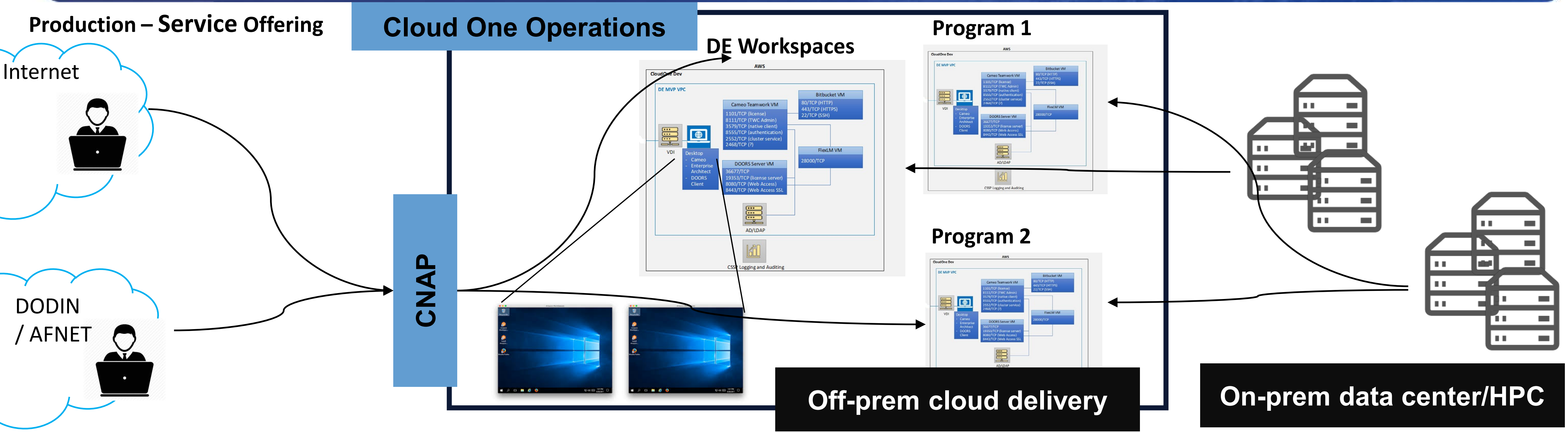
Service Desk Support

- Tier 1, Tier 2, Tier 3
- DE Tool Support

CLOUD ONE

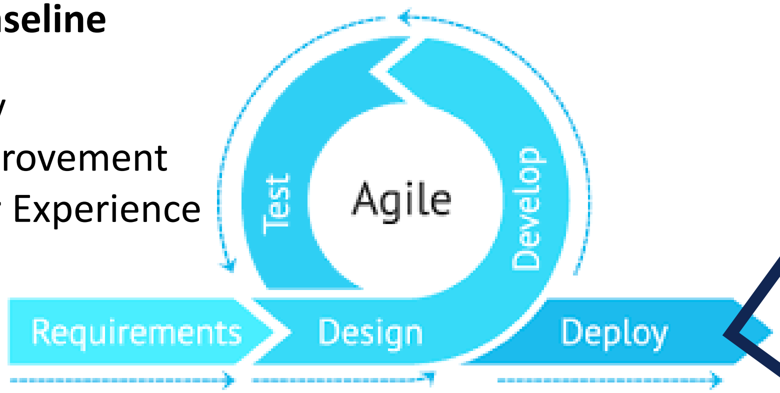
FAST
SECURE
STREAMLINED

DE Service Concept Evolution



Development Baseline

- Agile Delivery
- Constant Improvement
- Focused User Experience



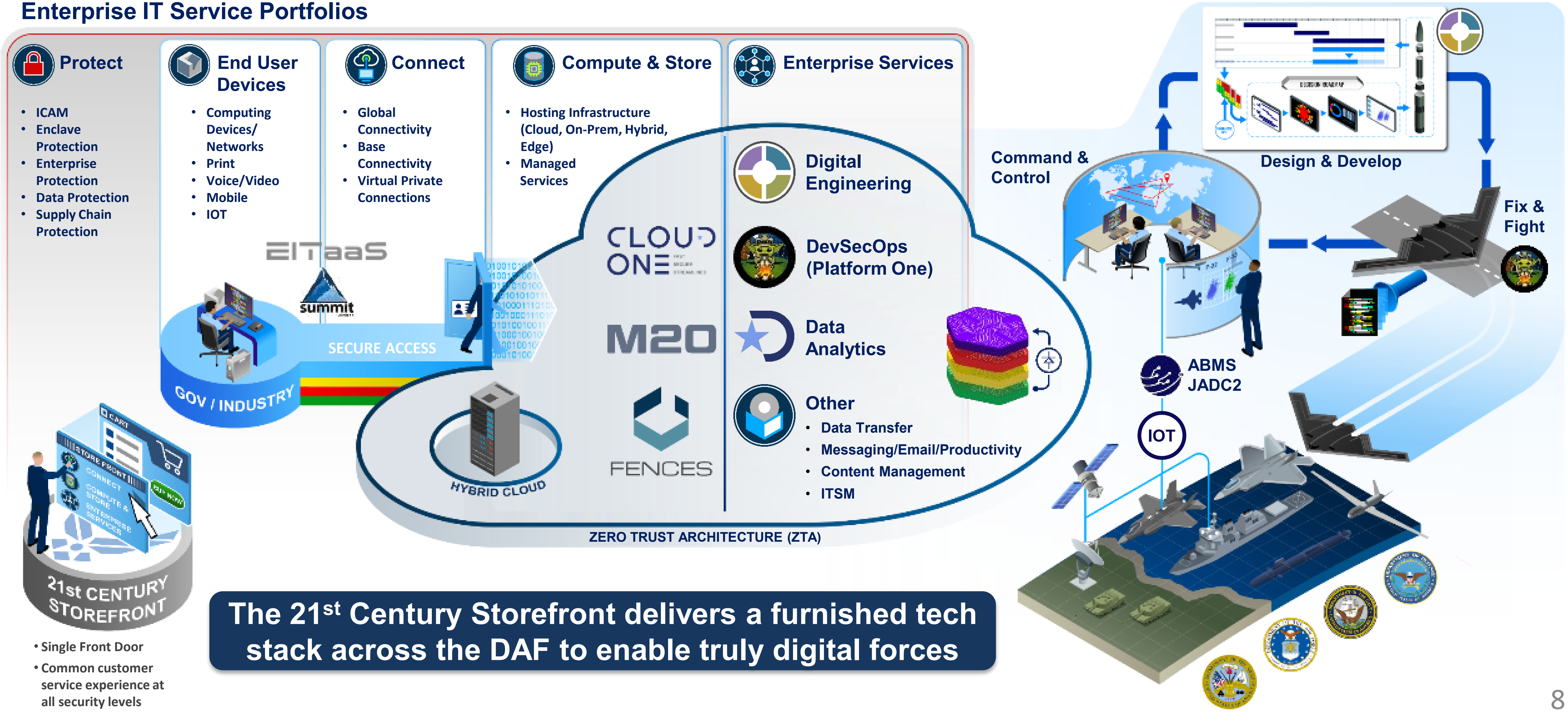
Containerize or Automate New Tools/Applications

DE Cyber Reference Model

Tool integration and Automation

Enterprise IT Services for the AF Digital Transformation

Enterprise IT Service Portfolios



Protect
- ICAM
- Enclave Protection
- Enterprise Protection
- Data Protection
- Supply Chain Protection

End User Devices
- Computing Devices/ Networks
- Print
- Voice/Video
- Mobile
- IOT

Connect
- Global Connectivity
- Base Connectivity
- Virtual Private Connections

Compute & Store
- Hosting Infrastructure (Cloud, On-Prem, Hybrid, Edge)
- Managed Services

Enterprise Services

Digital Engineering

DevSecOps (Platform One)

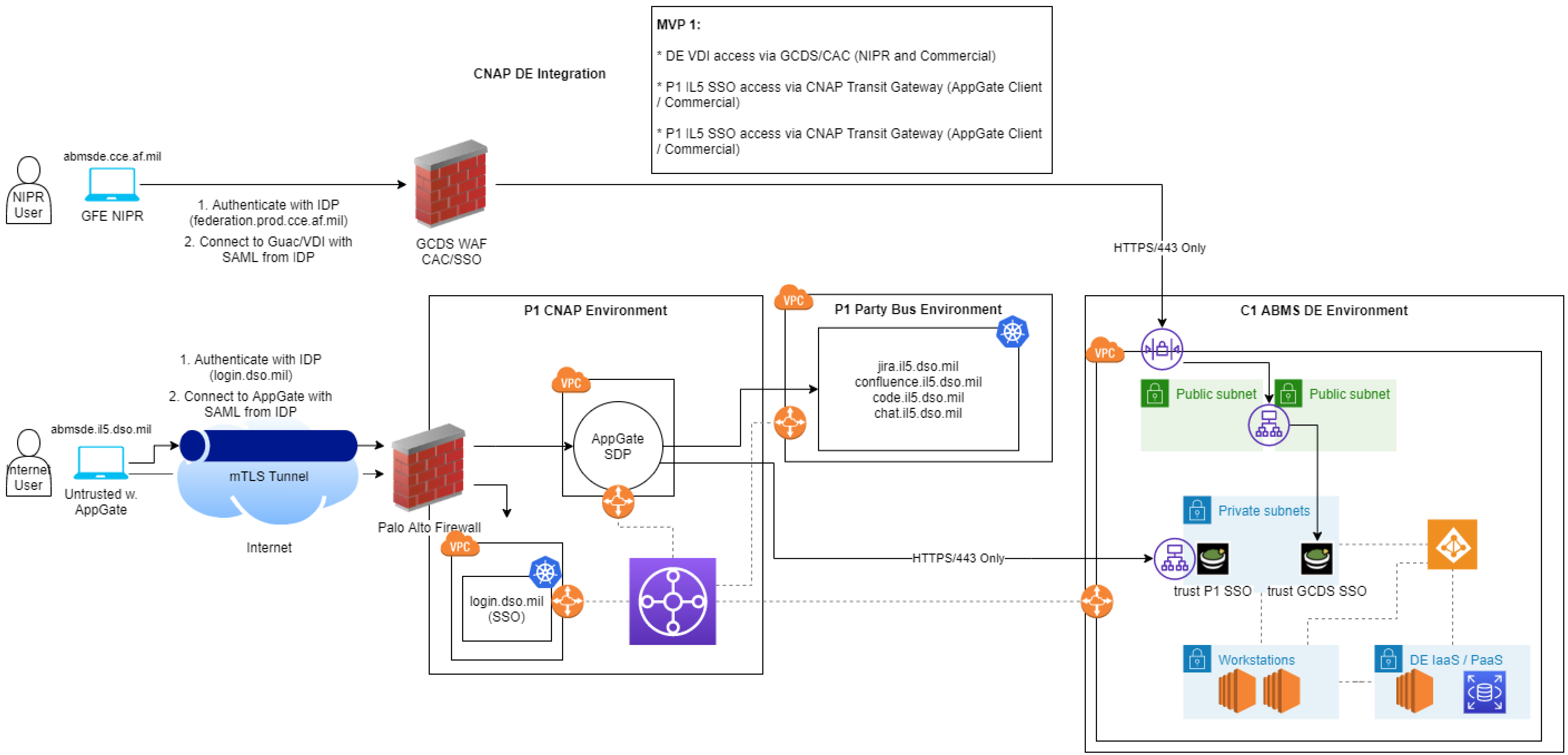
Data Analytics

Other
- Data Transfer
- Messaging/Email/Productivity
- Content Management
- ITSM

- Single Front Door
- Common customer service experience at all security levels

The 21st Century Storefront delivers a furnished tech stack across the DAF to enable truly digital forces

Integration



MVP 1:

* DE VDI access via GCDS/CAC (NIPR and Commercial)

* P1 IL5 SSO access via CNAP Transit Gateway (AppGate Client / Commercial)

* P1 IL5 SSO access via CNAP Transit Gateway (AppGate Client / Commercial)

Department of the Air Force

Integrity - Service - Excellence

DoD Enterprise DevSecOps Initiative & Platform One CoP Presentation

Mr. Nicolas Chaillan
DAF Chief Software Officer
Co-Lead, DoD Enterprise DevSecOps Initiative
Chair, DSAWG DevSecOps Subgroup

V1.0 – UNCLASSIFIED

CSO Website – Continuously Updated!

- Want to find information about the DevSecOps initiative and the CSO?
  - **Our latest documents/videos:** https://software.af.mil/dsop/documents/
  - **Our latest training videos/content at:** https://software.af.mil/training/
  - **Platform One Services:** https://software.af.mil/dsop/services/
  - More information about :
    - Platform One: https://p1.dso.mil
    - Cloud One: https://software.af.mil/team/cloud-one/
    - Repo One: https://repo1.dso.mil
    - Iron Bank: https://ironbank.dso.mil
    - Registry One: https://registry1.dso.mil
    - DevStar: https://software.af.mil/dsop/dsop-devstar/
    - Our Events/News: https://software.af.mil/events/

PLATFORM ONE
SMOKEY
WATERFALL, ONLY YOU CAN PREVENT

PLATFORM ONE | METRICS

ORGANIZATION

4	MILITARY
14	CIVILIAN
225+	CONTRACTORS
25+	COMPANIES
34	TOTAL CONTRACTS

BIG BANG

DEPLOYMENT PACKAGES

- GBSD
- F-35
- ARMY INSCOM
- CYBER COMMAND
- GPS OCX
- EDGEONE
- 76TH SWEG

COLLABORATION TOOLS

ACTIVE USERS

11,196	19,329
DAILY	MONTHLY

IRON BANK

454 CONTAINERS

PARTY BUS

3,210	PRODUCT DEVELOPERS
2,557	MICROSERVICES
41	APPS IN PRODUCTION
209	PRODUCT TEAMS

CNAP

20,200
AVG. UNIQUE ALLOWED IPS

DORA

20.8 COMMITS PER DAY

- <2 DAYS FOR LEAD TIME
- 15 MIN TO RESTORE
- <5% CHANGE FAILURE RATE

Platform One Multi Tenant DevSecOps Managed Service

- **Party Bus - ABMS All-Domain Common Environment**
  - Platform One Shared Enterprise DevSecOps Environments (Multi-Tenant)—for Development, Test, and Production
  - Multi-Cloud/Multi-Classification: Cloud One, SC2S, C2S, and FENCES
  - These are DevSecOps environments that benefit from the Platform One cATO managed by the Platform One team as multi-tenant environments
  - Provides Continuous Integration / Continuous Delivery (CI/CD) and various development and project management tools/capabilities
  - Impact Level (IL)-2 to IL-6 and TS/SCI / SAP environments exist or being built for ADCE
  - Designed to be environment agnostic (including clouds and edge/datacenter deployments)—supports AI/ML use cases and elasticity
  - CNAP allows for internet-facing access with its “baked-in” Zero Trust security/architecture

Platform One Anywhere!

- **Big Bang - Platform One Dedicated DevSecOps Environments**
  - Instantiate a dedicated DevSecOps environment—on air-gapped environments, edge, embedded systems or cloud environments—with a push-button deployment using GitOps/Infrastructure as Code to ensure scalability and no drift between environments/classifications
  - Could be instantiated on CMCC to enable CI/CD and Kubernetes/containerized workload on the existing RCO capability
  - Build, deliver and operate custom Infrastructure as Code and Configuration as Code with the deployment of a dedicated DevSecOps environment at any classification level with CI/CD pipelines and c-ATO
  - Can be deployed anywhere (edge, cloud, air-gapped etc.) including for hardware in the loop testing.
  - Check it out: https://repo1.dso.mil/platform-one/big-bang

Platform One Enables Edge Use Cases

- Platform One Big Bang can be deployed on any environment. We have ongoing pilots with RTOS.
- Big Bang has been deployed successfully for On-Ramp 4 (NIPRNet) in Germany and ShOC (Shadow Operations Center) near Nellis AFB (Hughes Center) incl SIPR.
- Big Bang is elastic and can adapt to CPU/memory/storage hardware availability.
- Multiple hardware options from HPE EdgeLine 8000 to Dell to Azure Stack and AWS Snowball/Outpost.
- HP EdgeLine EL8000, example:
  - Four blades
  - CPU: 24 core 2.4 GHz Intel processor
  - RAM: 192 GB
  - GPU: NVIDIA T4
  - SSD: 2x 256GB SSD
  - NVME: 4x 2TB NVME

Platform One Enables Cross Domain with Baked-In Security

- **Stargate: Diode/CDS**
  - Provided as a managed service by Platform One (Launch in April 2021).
  - Bring a “pre” and “post” landing zone compliant with NSA requirements to push artifacts to the high side including containers
  - Approved for use with AWS Diode
  - Assesses cybersecurity risk and analyzes Bill of Material (BOM) and enforces provenance (cert based) and integrity (checksum)
- **vSOC: Virtual Security Operations Center**
  - Brings Data Lake/Warehouse capability with Elasticsearch, Fluentd, Kibana (EFK)
  - Cloud agnostic, Kubernetes native
  - Brings Security Information and Event Management (SIEM)
  - Brings Security Orchestration, Automation and Response (SOAR) capabilities
  - Leverages behavior detection and not just CVEs/signature scanning

Platform One
Data Feeding/Streaming Capabilities

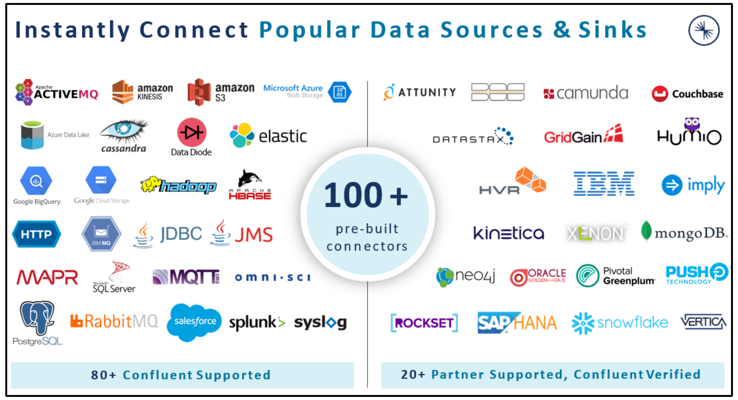
- Leverages Kafka (Confluent) with FIPS compliant crypto to bring a streaming capability for data ingestion, ETL, Pub/Sub.
- Leverages KSQL for micro-services level databases
- Connects to CNAP and P1 SSO/PKI

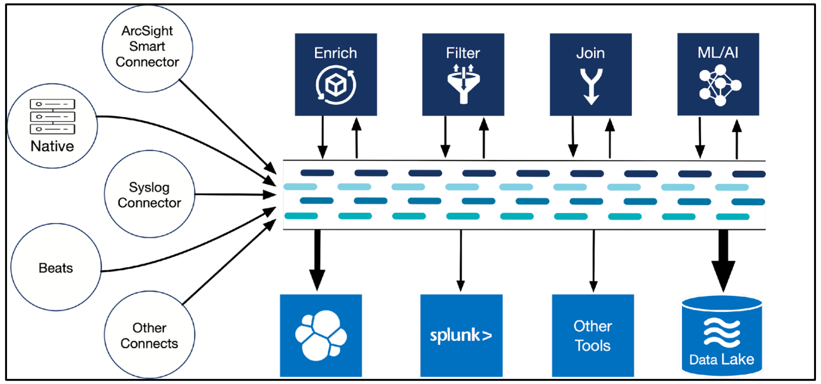
Mission Ready Kafka

Security
- RBAC
- Structured Auditing
- FIPS 140-2
- Secrets Protection

Resilience
- Multi-region replication and failover
- Auto data balancing
- Confluent Support

Operations
- Control Center
- Ansible Automation
- Kubernetes Operator
- Confluent Support

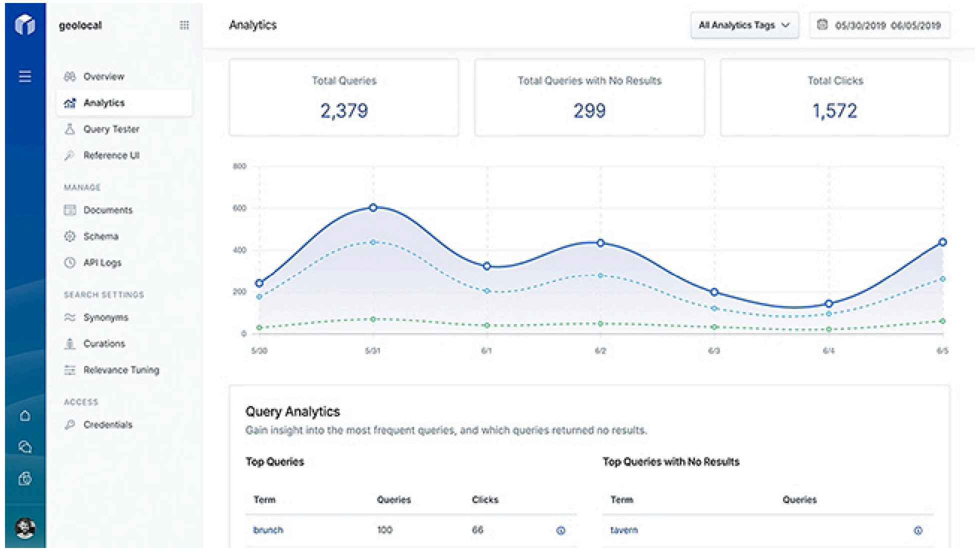


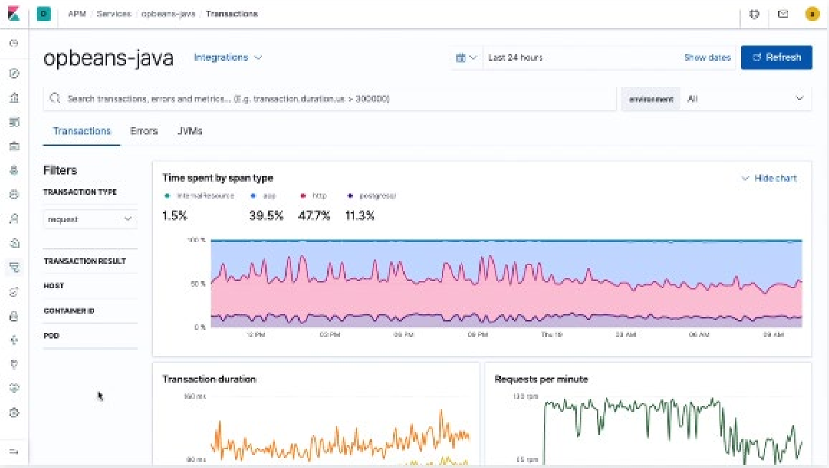


- Cloud agnostic, air-gapped capable, elastic
- 100+ pre-built connectors
- Launched On-Ramp 4.

Platform One Data Capabilities

- Leverages Elastic with FIPS compliant crypto to bring a data lake/warehouse and ETL capabilities
- Brings visualization, observability, federation, aggregation etc.
- Used as a centralized logs/telemetry stack and SIEM capability.





- Cloud agnostic, air-gapped capable, elastic
- Customized dashboards and connectors

Platform One Critical Core Infrastructure Services

- **Full details at: https://software.af.mil/dsop/services/**
- **Identity Management / SSO / PKI**
  - Provided as a managed service by Platform One.
  - Brings Single Sign On with various DoD PKI options and MFA options.
  - Brings Person Entity (PE) and Non Person Entity (NPE) x509 certificate based authentication
  - Connects to existing AF, DoD and DIB PKI capabilities
  - Provide secure and cloud native, agnostic and elastic capability
  - Leverages VAULT capability and provides automated certificate generation, Kubernetes native and allows for automated certificate rotation
  - Can be used for code signing, container signing and NPE/PE auth
  - Centralizes/Aggregates logs and pushes to CSSP and vSOC

Platform One Critical Core Infrastructure Services

- **Registry One - DoD Container Registry**
  - 300+ containers available.
  - Registry One is the DoD registry of digitally signed, binary container images (both FOSS and COTS) that have been hardened by Iron Bank. Containers accredited have DoD-wide reciprocity across classifications.
  - Registry One is currently operated at https://registry1.dso.mil/.
- **Cloud Native DNS**
  - Provided as a managed service by Platform One.
  - Cloud-native, agnostic and elastic DNS capability with .MIL and non .MIL capabilities
  - Fully managed by configuration as code and Git mergers
  - Runs on Kubernetes using coreDNS.

Platform One Enables Connectivity With Zero Trust Architecture

- **Cloud Native Access Point (CNAP): Zero Trust Architecture**
  - Provided as a managed service by Platform One
  - Brings a full Zero Trust stack enforcing device state, user RBAC and Software Defined Perimeter/Networks based on Google BeyondCorp concepts
  - Can be deployed air-gapped and on classified environments
  - Allows access to Cloud One (AWS GovCloud and Azure Government) and Platform One without having to go through the DISN/DoDIN/CAP/IAP
  - Allows access from thick clients on BYOD, government owned devices (both mobile and desktop) while enforcing their device states by using AppGate as a zero trust client
  - Allows for VDI options for zero / thin clients
  - Brings DMZ/Perimeter stack with break and inspect, IDS/IPS, WAF capability, full packet capture as an elastic Cloud based stack
  - Brings Single Sign On with various DoD PKI options and MFA options
  - Centralizes/Aggregates logs and pushes to CSSP and vSOC

Thank You!

Nicolas Chaillan
Chief Software Officer, U.S. Air Force
af.cso@us.af.mil – https://software.af.mil

PEO Roadshows

Software Acquisition Pathway and SW Modernization

Scaling DoD's Software Transformation

Sean Brady

DoD Senior Lead for SW Acq

USD(A&S)/Acq Enablers

https://aaf.dau.edu/aaf/software/

PEO Roadshows for 5000.87 & SW Modernization

- Acquisition Enablers & SW Modernization SSG Outreach Campaign
  - directly interface with the field
  - listen to learn
  - remove their impediments/red-tape
  - enable their adoption of 5000.87 SW Pathway & DevSecOps
- Preliminary set of PEOs lined up
  - cloud-native
  - cyber-physical weapons
- PEOs: please offer this opportunity to your PEO network
  - We'll partner on tailored events for their needs (e.g., Cloud/cATO adoption)

5000.87 & DevSecOps together, provide the modern framework that prioritizes speed and adaptability for digital product delivery across all Warfighting domains. Let's enable the transformation.

Example Agenda

- WHO:
  - **Army PEO STRI** (in partnership with PEO AVN): ~150+ members
  - A&S/Acquisition Enablers and the SW Modernization SSG
- WHAT:
  - 5000.87 SWP: 60 minutes
  - SW Mod Topics that enable .87 (DevSecOps; Cloud; cATO): 30 minutes
- WHY:
  - PEO STRI wants to modernize & navigate the AAF/Software Acq Pathway
- WHEN:
  - Tuesday 23 Feb
  - **90 minutes**
- WHERE:

MSFT Teams

Example of real-world roadshow already conducted

Potential Future PEOs

- WHO:
  - Army **PEO Aviation** and **PEO Missiles & Space**
  - A&S/Acquisition Enablers and the SW Modernization SSG
- WHAT:
  - AAF: 30 min
  - 5000.87 SWP: 60 min
  - Dev*Ops and Embedded Weapon Systems: 30 min
- WHY:
  - PEOs want to understand AAF and the .87 SWP and
  - how .87's attendant processes can work in their embedded and safety-critical domain
- WHEN:
  - Apr 2020
  - 120 min

Example of planned roadshows

Establish guidelines appropriate for embedded and real-time safety critical software development; will target PEO AVN

PEO Roadshows

Software Acquisition Pathway and SW Modernization

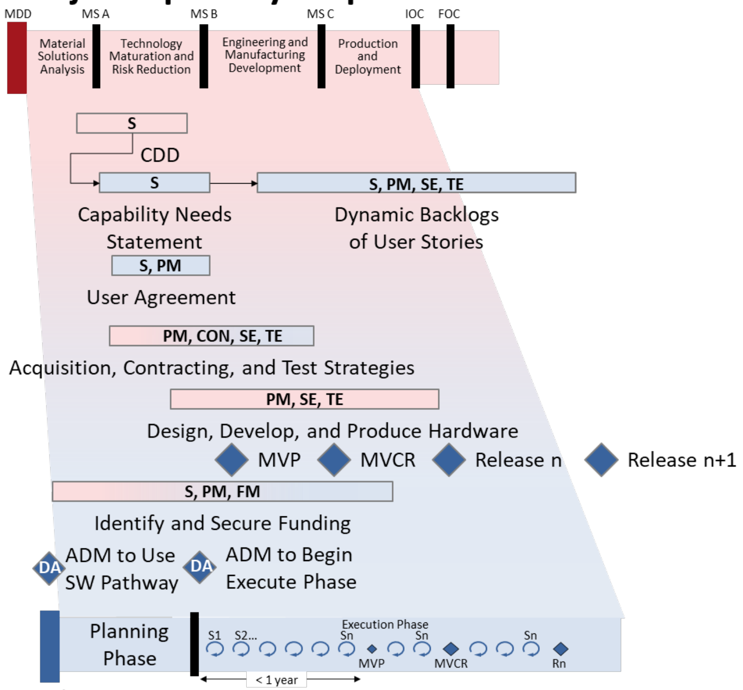
Optimizing .87 for Weapons and Dev*Ops

Sean Brady / DoD Senior Lead for SW Acquisition

Nicolas Chaillan / AF Chief Software Officer / Dev*Ops Lead

Kyle Fox / GBSD Chief SWE

Major Capability Acquisition


MDD
MS A
MS B
MS C
IOC
FOC
Material Solutions Analysis
Technology Maturation and Risk Reduction
Engineering and Manufacturing Development
Production and Deployment
S
CDD
S
Capability Needs Statement
S, PM, SE, TE
Dynamic Backlogs of User Stories
S, PM
User Agreement
PM, CON, SE, TE
Acquisition, Contracting, and Test Strategies
PM, SE, TE
Design, Develop, and Produce Hardware
MVP
MVCR
Release n
Release n+1
S, PM, FM
Identify and Secure Funding
DA
ADM to Use SW Pathway
DA
ADM to Begin Execute Phase
Planning Phase
Execution Phase
S1
S2...
Sn
Sn
Sn
MVP
MVCR
Rn
< 1 year

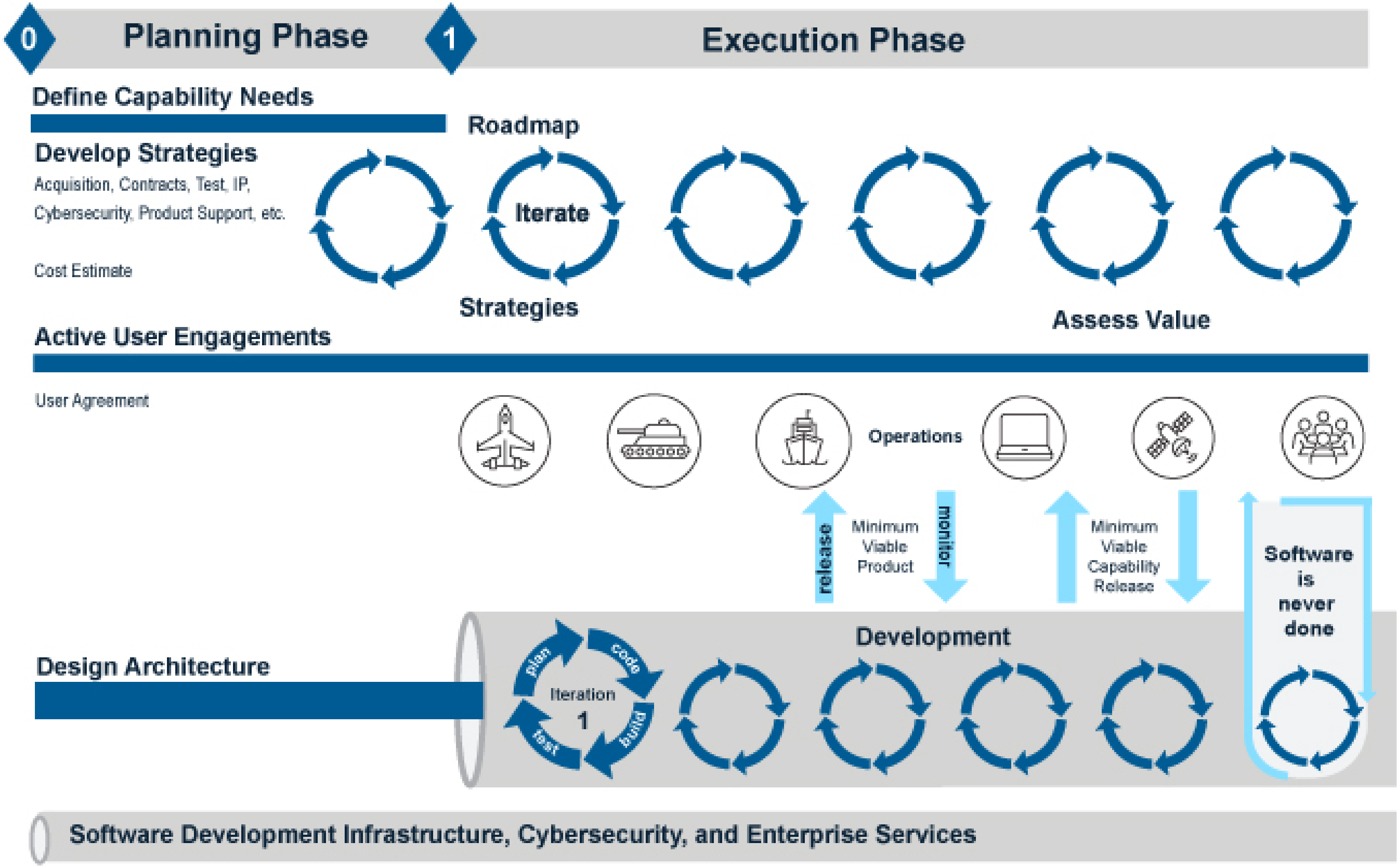
Software Acquisition

Continuous Development *hours - days*	T_K = (Dev)	
Continuous Integration *2 weeks – 1 month*	T_{K+1} = (Dev)(Ops)	← Industry culture and policy evolved; blurred lines between dev and ops environments
Continuous ATO *+ hours*	T_{K+2} = (Dev)(Sec)(Ops)	← Security culture and policy evolved; baked elements into automated pipeline
Continuous Safety *+ months*	T_{K+3} = (Dev)(Sec)(Safety)(Ops)	Must evaluate and evolve these elements (and more) to enable automated pipeline
Continuous Airworthiness *+ months*	T_{K+4} = (Dev)(Sec)(Safety)(AW)(Ops)	
Continuous Test *+ years*	T_{K+5} = (Dev)(Sec)(Safety)(AW)(DT/OT)(Ops)	
Continuous Weapons *+ months*	T_{K+6} = (Dev)(Sec)(Safety)(AW)(DT/OT)(Seek Eagle)(Ops)	
Continuous Nuclear *+ months*	T_{K+7} = (Dev)(Sec)(Safety)(AW)(DT/OT)(Seek Eagle)(Nuc)(Ops)	
...	T_{K+n} = (Dev)*(Ops)	

Keys to Success:

1. Evolve culture and policy
2. Early stakeholder involvement
3. Automated vs. manual processes

Software Acquisition Pathway



https://aaf.dau.edu/aaf/software/

Ignite Innovation and Execution

Partner with Services and Joint Staff to streamline and tailor <u>requirements</u> processes for software

Partner with Services and CAPE to streamline and iterate on software <u>cost estimation</u>

Partner with Services and DOT&E, DT&E to modernize, integrate, and automate software <u>T&E</u>

DoD Services/Agencies Empowered and Directed to Align and Streamline Processes

How can YOU make .87 an effective tool for your PEO?

Policies	• DODI 5000.87 signed Oct 2020 • Most Functional DODIs signed • Working with Services to update their SWP policies
Program Support	• A&S/SWP Team advising programs on navigating SWP • Identifying systemic issues & working WITH them: • AE consulting getting results; request 1 v 1 consulting w/ us • breaking down barriers; crafting innovative strategies • Need more SAE and PEO staff involvement
Awareness Training	• Train your workforce: adopt PEO roadshows, webinars, training, and AMAs for all members of enterprise (REQ/TEST/COST/FM/PM/et al.) • We offer tailored .87 training (e.g. JS, PMOs, DAU, NDU, JAIC) • DAU Agile/Cloud/DevSecOps Academy offerings • Developing Digital DNA course for novel SW training
Guidance & Templates	• Evolving SWP guidance on AAF website • Evolving and adding SWP templates • Contribute breakthroughs & real-world vignettes especially in key areas: requirements/estimation/T&E and “Ignite” reform projects

https://aaf.dau.edu/aaf/software/

How can YOU make .87 an effective tool for your PEO?

Policies	• DODI 5000.87 signed Oct 2020 • Most Functional DODIs signed • Working with Services to update their SWP policies
Program Support	• A&S/SWP Team advising programs on navigating SWP • Identifying systemic issues & working WITH them: • AE consulting getting results; request 1 v 1 consulting w/ us • breaking down barriers; crafting innovative strategies • Need more SAE and PEO staff involvement
Awareness Training	• Train your workforce: adopt PEO roadshows, webinars, training, and AMAs for all members of enterprise (REQ/TEST/COST/FM/PM/et al.) • We offer tailored .87 training (e.g. JS, PMOs, DAU, NDU, JAIC) • DAU Agile/Cloud/DevSecOps Academy offerings • Developing Digital DNA course for novel SW training
Guidance & Templates	• Evolving SWP guidance on AAF website • Evolving and adding SWP templates • Contribute breakthroughs & real-world vignettes especially in key areas: requirements/estimation/T&E and “Ignite” reform projects

https://aaf.dau.edu/aaf/software/

Cultural Barriers for DoD Software

Risk aversion a huge risk in DoD acquisition.

Getting key functional stakeholders onboard early is critical to adopt Agile/DevSecOps via radical new ways than traditional acquisition.

How can you **overcome cultural roadblocks** in your organization to enable rapid software delivery?

Question to the CoP

- Q1: Is anyone aware of a business case analysis we can show programs as an example of the cost/time savings of using Cloud One/Platform One as enterprise services vs the cost/time to build cloud/platform infrastructure for an individual program?

- Q2: Has anyone done an analysis of enterprise service vs on-prem?

Next DevSecOps CoP Meeting

- Date/Time: Thursday, April 8th, 2021 from 1:00 PM until 4:00 PM ET

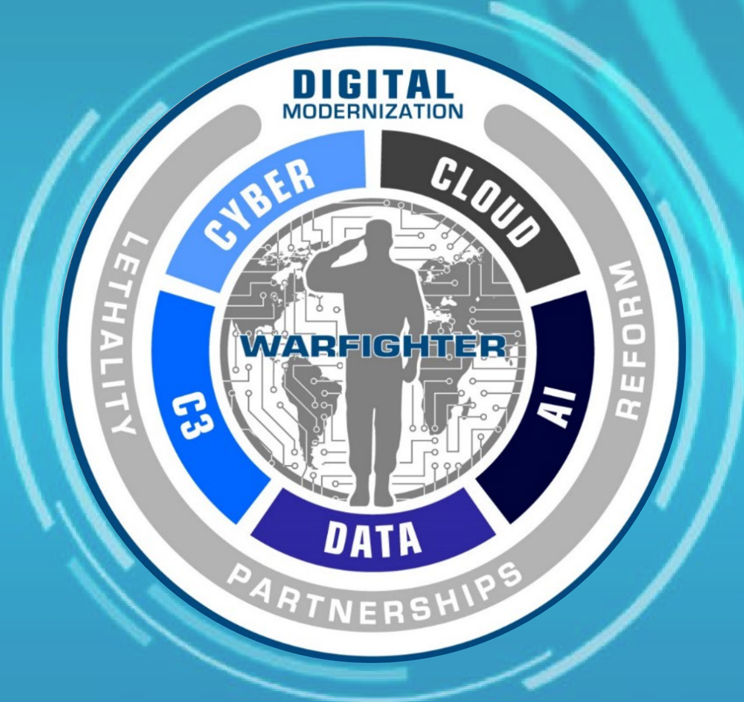
- Tentative Agenda:
  - Software Modernization Strategy – DoD CIO
  - Testing Automation – Army ISEC
  - Cyber.mil – DISA

Closing Remarks

Contact Information

DevSecOps Mailbox	osd.devsecops@mail.mil	
MilSuite Site	https://www.milsuite.mil/book/groups/dod-enterprise-devsecops	
Air Force Site	https://software.af.mil/	
Nicolas Chaillan	Air Force	nicolas.chaillan@us.af.mil
Jeff Boleng	OUSD(A&S)	jeffrey.l.boleng.civ@mail.mil
Rob Vietmeyer	DoD CIO	robert.w.vietmeyer.civ@mail.mil
Ana Kreiensieck	DoD CIO	ana.i.kreiensieck.ctr@mail.mil
Michael Savage	DISA	michael.s.savage2.civ@mail.mil

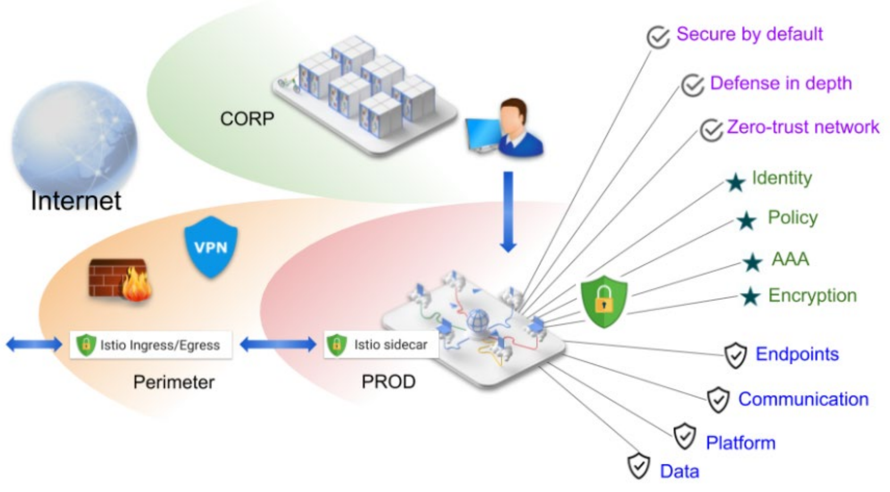
QUESTIONS?


DIGITAL
MODERNIZATION
CYBER
CLOUD
LETHALITY
REFORM
WARFIGHTER
C3
AI
DATA
PARTNERSHIPS

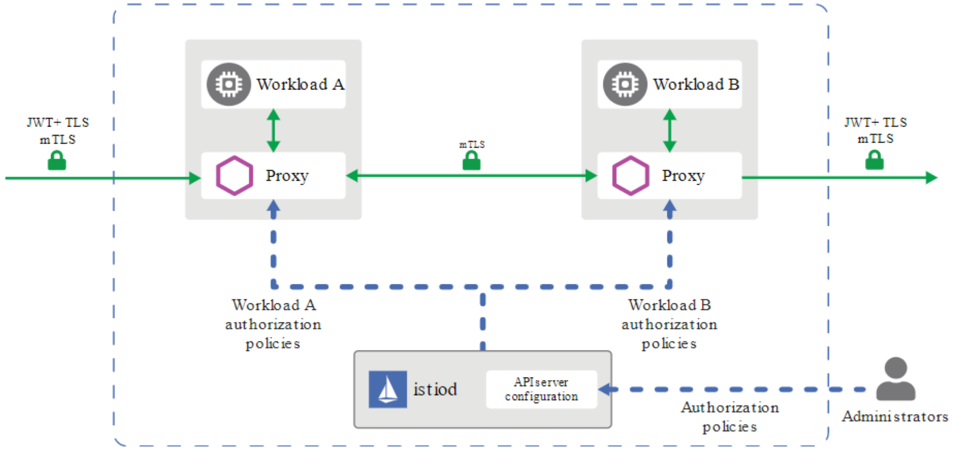
Backup Slides

Zero Trust: Service Mesh (ISTIO)

- Brings Zero Trust for East/West traffic across systems using NPE cert-based authentication.
- ISTIO sidecar proxy, baked-in security, with visibility across containers, by default, without any code change
- Benefits:
  - Zero Trust model: East/West Traffic Whitelisting, ACL, RBAC…
  - mTLS encryption by default, Key management, signing…
  - API Management, service discovery, authentication…
  - Dynamic request routing for A/B testing, gradual rollouts, canary releases, resilience, observability, retries, circuit breakers and fault injection
  - Layer 7 Load balancing



Istio Security Overview



Authorization Architecture

Platform One Critical Core Infrastructure Services

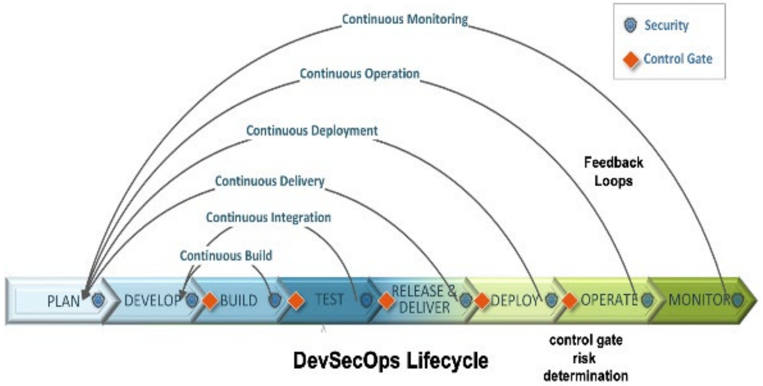
- **Repo One - DoD Centralized Container Source Code Repository (DCCSCR)**
  - Container source code, Infrastructure as Code, K8S distributions, etc.
  - Repo One is the central repository for the source code to create hardened and evaluated containers for the Department of Defense. It also includes various source code open-source products and infrastructure as code used to harden Kubernetes distributions.
  - Repo One is currently operated at https://repo1.dso.mil/dsop/.
- **Iron Bank - DoD Centralized Artifacts Repository (DCAR)**
  - 300+ containers available.
  - Iron Bank is the DoD repository of digitally signed, binary container images (both FOSS and COTS) that have been hardened according to the Container Hardening Guide. Containers accredited in Iron Bank have DoD-wide reciprocity across classifications.
  - Iron Bank is currently operated at https://ironbank.dso.mil/.

Continuous Risk Monitoring
Continuous Risk Determination

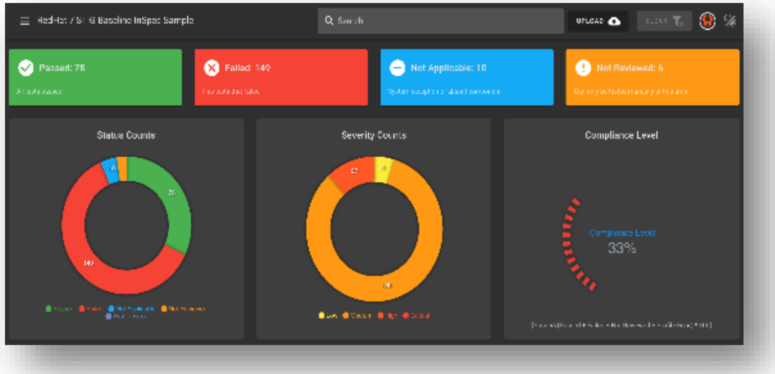
- Key points:
  - Move away from snapshot in time towards auto-generated content displayed in a dashboard showing risk posture in real-time
  - Extensive utilization of SW reuse, reciprocity, & inheritance from underlying infrastructure, platform, SW Factory, and authorized-to-use functional components
  - CI/CD security findings that exceed the risk threshold trigger an event to involve ISSM, assessor or AO then put on the backlog for remediation scheduling in future sprint
  - Continuous validation of security configuration hardening and implementation of controls
  - Use of IaC to create a consistent, secure, and repeatable instance of application support infrastructure
  - Execution of SW Product within a secure authorized Platform based on the DoD CIO Enterprise DevSecOps Reference Design

Through the execution of these practices, the SW Product has been through an automatic risk determination based on the AO's prescribed risk tolerance resulting in the SW Product **automatically authorized for use**

control gates risk tolerance checks



Security Posture Visualization


RedHat / STIG Baseline InSpec Sample

Passed: 78

Failed: 149

Not Applicable: 10

Not Reviewed: 6

Status Counts

Severity Counts

Compliance Level

Compliance Level 33%

Result: continuous risk analysis, risk determination, and authorization

Backup Slides

Software Requirements

- FY20 NDAA Exempted SWP programs from JCIDS
  - Until VCJCS, USD(A&S), and SAEs agree on new process
- Further codified in DODI 5000.87
  - Use Capability Needs Statement (CNS), roadmaps, backlogs
- Services responsible for new, streamlined processes
- Joint Staff updating JCIDS Manual this month

JCIDS IGNITE

Services, A&S, and JS need to collaborate on a new, streamlined model for SW requirements

Software Independent Cost Estimates

- DODI 5000.73 requires CAPE ICE for SW > ACAT II
  - 210 days for an ICE is too long for SW timelines
- Lifecycle estimates (IOC + x) vs Software is never done
- Need to streamline cost artifacts like CARD for SWP
- Full Funding requirement constraints
- Need to modernize cost estimating for SW practices

Service Cost Agencies, A&S, and CAPE need to collaborate on a new cost models for software

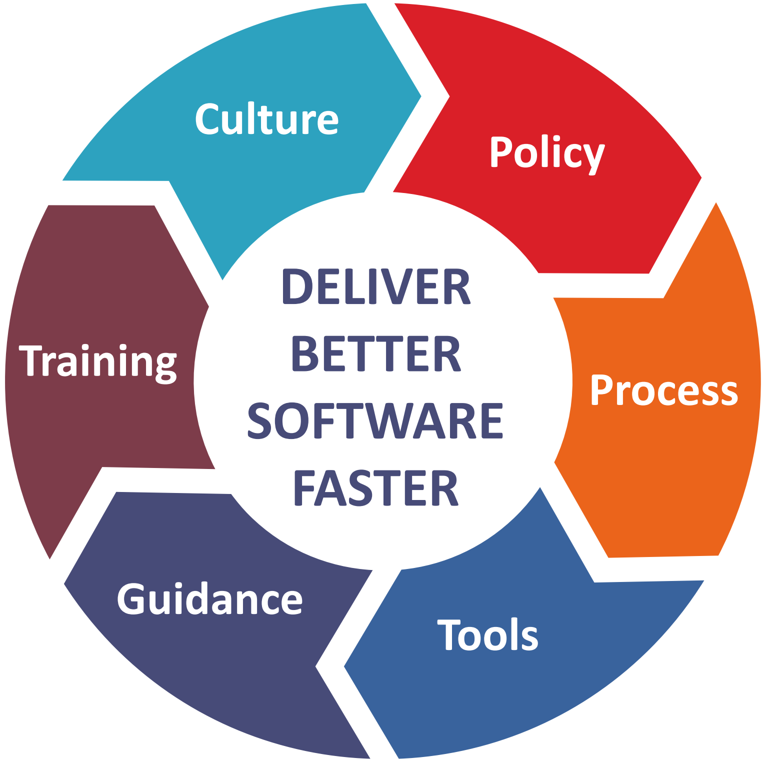
Software T&E

- T&E and ATO timelines do not support modern SW
  - Accelerate to days or hours to enable continuous delivery
- Software T&E Strategies, TEMPs – content, approvals
- Increasing automation and user engagements
- Rethinking, integrating contractor test, DT, OT
  - Shifting T&E left and shifting OT right
- T&E in DevSecOps and cloud-native environments

T&E Ignite

Services, A&S, R&E, DOT&E need to collaborate on a new T&E models for software

Strengthening DoD Software Acquisition



BETTER

- High Mission Value
- Cyber Secure
- Enable Efficiencies

FASTER

- Lead Time – Need to Delivery
- Frequency of Releases
- Rapid Response to Operations/Cyber

CULTURE
Human-centered design, speed of delivery, and continuous improvement

POLICY
OSD, Joint Staff, and Service policies to provide flexible structure for modern software

PROCESS
Streamline and transform cost, requirements, T&E, cyber, and sustainment for software

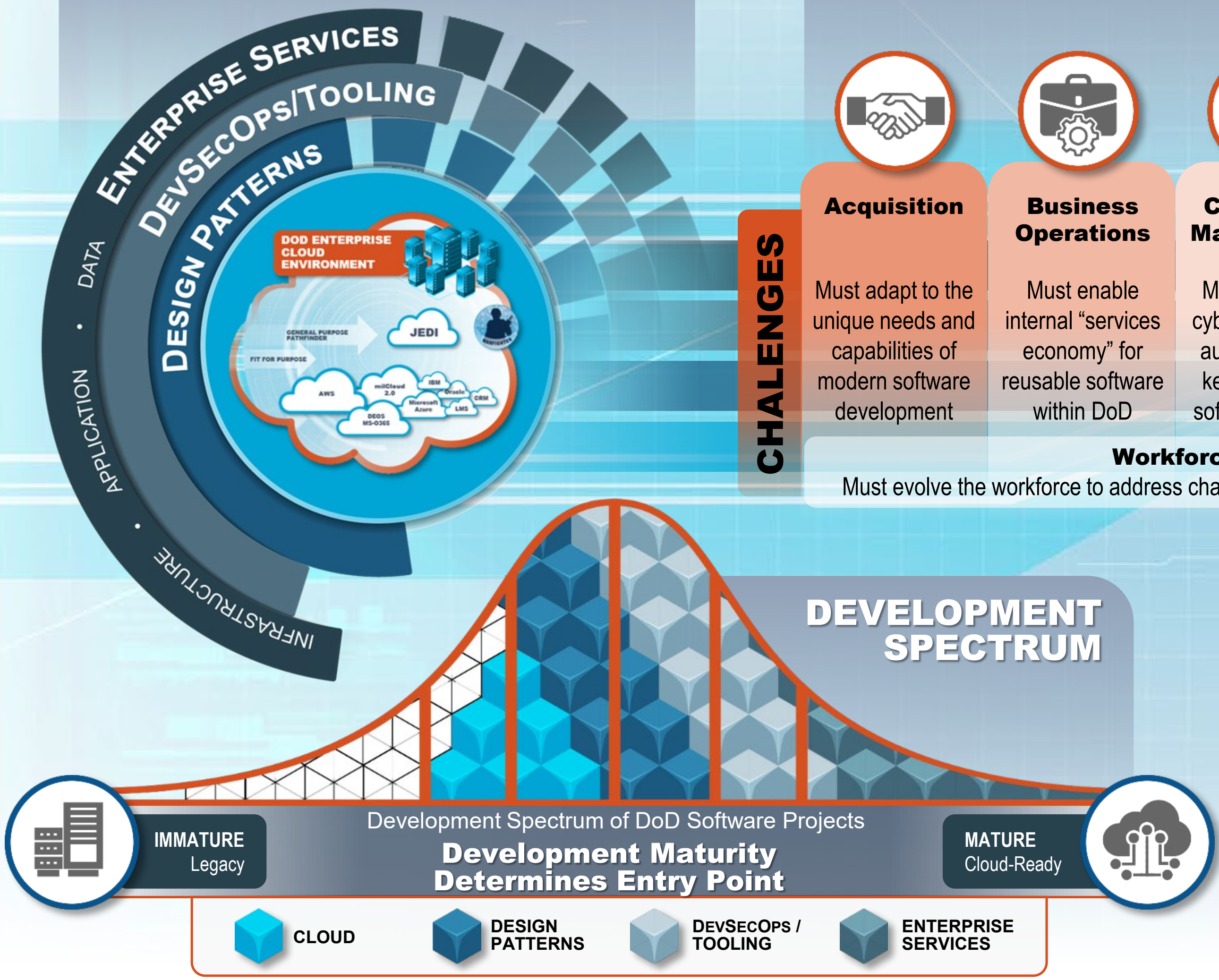
TRAINING
Transform software training for DoD's acquisition and operational workforces

GUIDANCE
Provide how-to insights and resources to shape program strategies and execution

TOOLS
Leverage software factories, DevSecOps pipelines, enterprise platforms, services

DOD SOFTWARE MODERNIZATION

Better Software Faster



Development Spectrum of DoD Software Projects

Development Maturity Determines Entry Point

PROCESS COMPONENTS

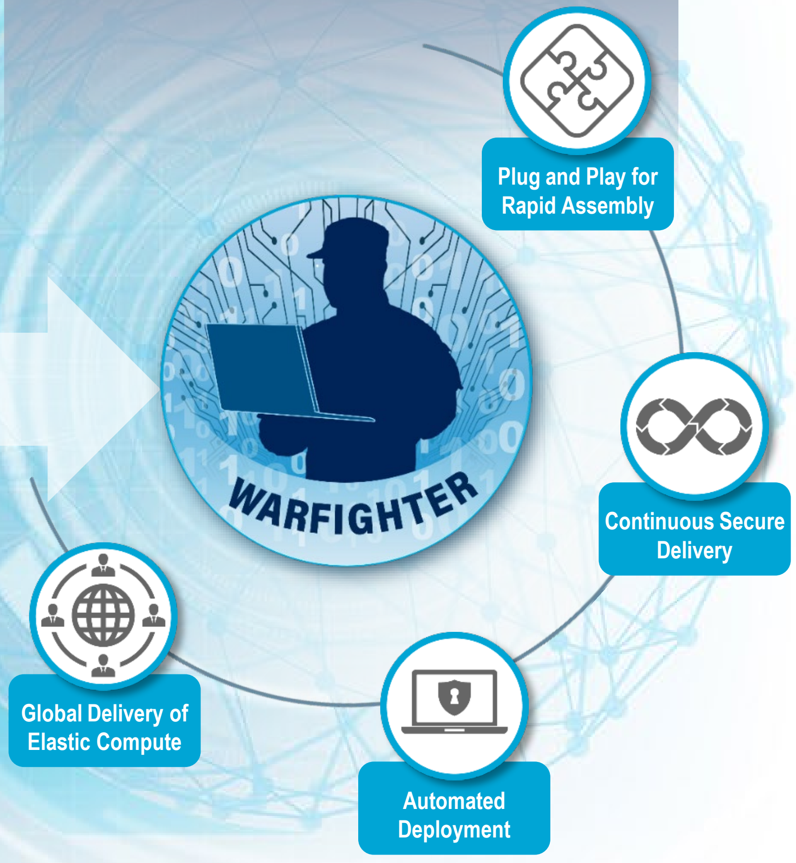
CHALENGES

Acquisition	Business Operations	Cyber Risk Management	Test and Evaluation
Must adapt to the unique needs and capabilities of modern software development	Must enable internal "services economy" for reusable software within DoD	Must automate cyber testing and authorization to keep pace with software delivery	Must bridge operational testing with software development

Workforce

Must evolve the workforce to address changes in process and technology

OUTCOMES


WARFIGHTER
Plug and Play for Rapid Assembly
Continuous Secure Delivery
Automated Deployment
Global Delivery of Elastic Compute