Compliance as Code for Big Bang
Risk Management Framework (RMF) Control Mapping to Accelerate Department of Defense (DoD) Authorization to Operate (ATO)

Platform One
AFLCMC/HNCX

This document approved for public release: distribution unlimited.
PA Case Number 66ABG-2022-0016. Refer all requests for information to AFLCMC/HNCX
Contents

• Why Platform One
• Why Big Bang
• Why OSCAL
• How OSCAL
Why Platform One
DoD Continually Falls Behind Adversaries in Software

Yet... all modern DoD systems including weapon systems are software-intensive systems

Build → Learn → Build ... takes too long...

<table>
<thead>
<tr>
<th>Activity</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fielding simplest, useful function</td>
<td>3 – 5 yrs</td>
</tr>
<tr>
<td>Testing complete system against side-effects</td>
<td>2 yrs</td>
</tr>
<tr>
<td>Testing cybersecurity via audit/penetration</td>
<td>2 yrs</td>
</tr>
<tr>
<td>Fielding high priority function</td>
<td>1 – 5 yrs</td>
</tr>
<tr>
<td>Fixing security holes</td>
<td>1 – 18 mos</td>
</tr>
<tr>
<td>Publishing software to use</td>
<td>1 – 18 mos</td>
</tr>
</tbody>
</table>

...and we still fail

94% Failed projects over $10M*

43% Utter and Complete Failures

51% Failed Expectations Over Budget Behind Schedule

*Standish Group CHAOS report
What is DevSecOps?

- **Continuous** software development with ops/sustainment w/security throughout
- Driven by the convergence of:
  - **Human-Centered Design** (HCD): a humanistic way to learn and work
  - **Commodity IT**: cheap, ubiquitous infrastructure = low-barrier of entry
  - **Agile**: *learning fast* to find solutions for complex/ill-defined challenges
Platform One: Why, How, What

**MISSION**
Accelerate Secure Software Delivery for the DoD.

**VISION**
A collaborative Defense Department enabled by continuous delivery

**Secure & Connect Users**
Cloud Native Access Point provides zero-trust security for development, test, and production enclaves

**Harden & Store Components**
DoD repository of hardened binary container images approved for DoD-wide use across enclaves

**Build & Deploy Platforms**
Infrastructure as Code (IaC) and Configuration as Code (CaC) deployable to cloud or on-premise infrastructures

**Code & Operate Apps**
DevSecOps Platform-as-a-Service at IL-2 to IL-4 accredited and managed by Platform One

---

DoD repository of hardened binary container images approved for DoD-wide use across enclaves

Infrastructure as Code (IaC) and Configuration as Code (CaC) deployable to cloud or on-premise infrastructures

DevSecOps Platform-as-a-Service at IL-2 to IL-4 accredited and managed by Platform One
Why Big Bang
3 Feb 2022 Continuous Authority to Operate (cATO)

• Issued by DoD Senior Information Security Officer
• Calls out specific guidance for cATO programs
  • Continuous Monitoring
  • Active Cyber Defense
  • Secure Software Supply Chain
• Big Bang is the Platform One starting point for a K8s-based platform that provides for Continuous Monitoring and Active Cyber Defense
  • Both inside Platform One, and used by third parties across the DoD as they wish
Architecture & Tools

Customer Repos

3rd Party Additions

Big Bang Addons

Big Bang Core

Vendor Cluster (RKE2, OCP, Konvoy)

Infrastructure (AWS, Azure, On-Prem)
Why OSCAL
The RMF/ATO “problem”

• Per GSA (18f):
  • “ATOs across government have traditionally taken 6-18 months, with a lot of slow back-and-forth between system owners and assessors.”

• Within the DoD, the RMF process is synonymous with the tools used to track controls
  • Manually intensive effort between tool experts and system experts called out by GSA

• Particularly with the advent of cloud software, control inheritance is of particular interest
RMF as a Hurdle to Adoption

- Big Bang is being deployed in different development and production environments across different services, both on-prem and in the cloud
  - Different customers (deployers) use different systems to manage the RMF process
  - Customers need to know what controls are inherited from Big Bang
    - Cannot afford 18 months of control entry!
- Big Bang releases a new version every 2 weeks
  - Did the answers to different RMF controls change?
- Our Solution: Distribute OSCAL control list with every version
  - Always up to date with version, and hopefully it works across systems
How OSCAL
Implementation Roadmap

• Map RMF controls to Platform One products
  • This was an intensive 2-day effort with some of our top engineers
  • Generated a mightily impressive Excel file

• Publish those controls in OSCAL format
  • This effort is ongoing
  • We have a few key stakeholders that we are working with to pilot this effort
    • Maybe some new ones in this venue?

• Integrate control mapping/OSCAL updates into the code release process
Control Mapping Layers

- **Infra** - The cloud/infra provides this control to the application directly
- **CNAP** - The CNAP provides this control to the application directly
- **IDP** - Control would be provided by using an Identity Provider
- **Distro** - Control would be provided by the Kubernetes distribution, which includes the OS/AMI
- **Org** - The organization implements the control outside of the tech stack
- **Self** - This package implements the control itself
- **N/A** - This control does not apply to this package
- **Package** - control is inherited from package
Proposed Updated Release Process

- In order to keep up to date, must be incorporated with the branch-merge workflow of the Big Bang Team
Questions?

Comments?