Where Our National Security Begins...
NRO
Industry Advisory Working Group
Working Session
April 30, 2019
Agenda

- Welcome & Introductions
- “Snapshots”
- “S2P Corner” & “C2S Corner”
- Action Team discussions
- Government Perspective
- Open Dialog
- No-Host Social
“Snapshots”

Upcoming Events

• GEOINT 2019: June 2-5
• Amazon Public Sector Summit: June 11-12
• Azure + AI Conference: June 11-13

May IAWG will be a “Peer Review” session 5/30
“C2S Corner”

Latest & Greatest…
Topics & Issues Discussion
Pre-Day: Public Sector AWSome Day
June 10, 2019, currently Waitlist.

13,000+ Expected Attendees
100+ Exhibiting Partners
160+ Sessions & Workshops

https://aws.amazon.com/summits/washington-dc/
“S2P Corner”

Latest & Greatest…

Topics & Issues Discussion

Explore on CWAN/JWICS @ https://jportal.S2P.proj.nro.ic.gov
NRO IAWG
Action Teams & Topics

• Agile & DevSecOps 2019
• NEW: Hybrid Cloud Business Model team
Agile & DevSecOps 2019
Focus Area Topics

1. Terms of Reference
2. Scaling Agile and DevSecOps across GED Program Offices
3. Contracting strategies, structures, and incentives
4. Training gaps, standardization, and program-specific implementations
5. ROI expectations and perceptions
6. E2E Mission Thread Closure in an Agile & DevSecOps world
NRO
Industry Advisory Working Group

Agile & DevSecOps 2019: Terms of Reference Team

Matthew Reider (Team Lead)

Ken Laskey       Jay Eward       Rob Manogue
John Farrell     Scott Lawler
Agile & DevSecOps 2019: Terms of Reference Team

**Challenge**

Different government, industry, and vendors use different terms of reference to describe similar things, or use same terms of reference to describe different things.

**Deliverable**

A document containing Terms of Reference and the source information in order to align government and industry.

**Approach**

1. Identify commonly used agile and DevSecOps terms across GED and NRO
2. Identify terms that have most divergent or misunderstood definitions
3. Identify major commercial and agile government sources of definitions to create matrix
4. Highlight those definitions or parts of definitions that enhance common understanding
**Solution Level Epics**
Definition: Multi-increment, multi-functional useful outcome that can be decomposed and allocated into multiple, single increment deliveries.
Example:
- OOS
- SRs: within Epic process data to generate products, accept support data for processing.

**Feature Level Epics**
Definition: Defines outcomes to a Project (e.g. OOS for M2C2) that delivers in a single increment (e.g. PI#1)
Example:
- GPF creates products IAW...

**Stories**
Definition: Decomposed functions into multiple iterations/sprints to accomplish increment outcome
- Typically will be over 2-4 week sprint/iteration timelines

**Solution Roadmap**
Represent the temporal view and planned delivery of Solution-Level Epics

**Program Roadmap**
Near term Project Level incremental features that support Solution-Level Roadmap

**Software Development Sprints/Iterations**
Graphics is UNCLASSIFIED
# Agile & DevSecOps 2019: Terms of Reference

## Agile Process Terms
- **Sprint**
- **Release**
- **User Story**
- **Story Point**
- **Story Point Normalization**
- **ScrumMaster**
- **Backlog Grooming/Refinement**
- **Test Driven Development**
- **Behavior Driven Development**

## Scrum
- **Scrum Meeting**
- **Sprint Review**
- **Sprint Demo**
- **Sprint Planning**
- **Product Owner**

## Potential Definition Sources
- Scaled Agile Framework for enterprise (SAFe)
- Agile Alliance “Agile Glossary”
- SmartSheet “Ultimate Agile Dictionary”
- 18F Agile Lexicon

## Organizational Terms
- **Culture**
- **Mindset**
- **Policy**
- **Risk Averse**

---

See Spreadsheet for Definitions
NRO
Industry Advisory Working Group

Agile & DevSecOps 2019:
Scaling DevSecOps across Programs

Marc Kriz (Team Lead)

Shawn Lucas        Pete Epstein        Eric Amberge
Themba Hinke       Sam Stollar         Joel Doyle
John Jeremiah       Kevin Chasse
Deliverable

Agile DevSecOps document/outbrief divided into 4 sections:

1. Introduction
2. Aspects of DevSecOps and their definitions
3. Key Enablers of Agile DevSecOps
4. Alignment with GED practices
Why is GED transitioning to an Agile culture and moving towards DevSecOps?

Establishing Secure Application Development capabilities will:

- Deliver applications in a secure and timely manner increasing the ability for GED to provide a competitive advantage to downstream customers
- Bake-in and enforce cybersecurity functions and policy from inception through operations
- Enhance enterprise visibility of development activities and reduce accreditation timelines
- Ensure seamless application portability across enterprise and mission program environments
- Drive GED transformation to Agile and Lean Software Development and Delivery
Alignment with GED practices

• **Manage** - Mentality: leadership and a view. What metrics will demonstrate to managers that the “mechanics of management” are different?

• **Expect what you inspect.** Mechanics don’t matter if no one cares about them.

• **Additional Best Practice to consider: Create 3-6 metrics**
  - Document historical benchmarks of progress and leading indicators of transformation.
  - If workforce knows what is being tracked, they will change behavior accordingly.
GED scaling Agile and DevSecOps across Program Offices
NRO
Industry Advisory Working Group

Hybrid Cloud Adoption & Business Model Action Team
Hybrid Cloud Action Team

Chris Arroyo (Team Lead)

Al Stewart         Robert Shelton         Keith Barber         Tim Stewart

DRAFT Problem Statement

Emergence of multiple providers with commercial cloud offerings presents the NRO with an opportunity to leverage a cloud agnostic environment ecosystem to maximize mission performance and business value. Without a good understanding of how to adopt business and operating models to fit the new paradigm, the government & industry base run the risk of unintended consequences that can detract from mission success. Additionally, lack of clarity and understanding from the government will inhibit industry’s ability to respond and may create disincentives that negatively impact the industry base.
Hybrid Cloud Action Team
Kickoff Summary

Objectives
• Define “Hybrid Cloud” and “Multi-Cloud” approaches in terms of business & programmatic model
• Identify potential business model ramifications, incentives and disincentives owing to government’s adoption of hybrid- and multi-cloud strategies

Challenges
• What doesn’t work today that could impact how the customer adopts a multi-cloud approach?
• What is the enterprise service approach? What is the data strategy? How are you servicing content to your end stream users?

Tasks
• How can the NRO utilize multiple clouds and what are our recommendations?
• Identify differences in business models that may unintentionally create winners and losers in the industry base
• Reconcile cloud contracting approaches and standardize terms and conditions across contracts
• Consideration of who decides which cloud(s) a program uses and in what proportion?

Outputs from Initial Meeting
• Need to define what is meant by “Hybrid Cloud” and “Multi-Cloud” in context of government program intent
• Focus on key tenets of Hybrid- and Multi-cloud programs, particularly on interoperability between clouds
• Identify best practices for selecting PaaS and SaaS solutions, particularly if offered by multiple cloud providers
• Collect insight from the NRO Tiger Team for action team consideration
NRO IAWG Action Team:
Accelerating Speed to Capability (STC)

Observations & Ideas

30 April 2019

Ben Chicoski (Team Lead)
Joe Chioda  Scott Lawler  Pete Epstein
Mike Moran  Ron Alford  Eric Viglione

Ben Chicoski
bchicoski@cloudbees.com
202.746.1124
Speed to Capability
Purpose / Overview

Our Task
- Identify process, development, and programmatic sources of delay to delivery of capabilities
- Make recommendations for concrete action. Operating principles:
  - Prioritize by need / impact
  - Be realistic – which needles can be moved?
  - Cite real-world examples from which to learn
- Iterate and refine based on Government-Industry feedback

Desired Outcomes
- a) Rapidly get new capabilities on contract, and then…
- b) Rapidly deliver approved, functional, relevant systems into users’ hands

Current Landscape
- Lack of incentives for prime contractors to realize faster delivery cycles
- Change processes biased toward status quo
- Increasing complexity of acquisitions in areas like IT causing skills gap in acquisition workforce
- Pilots that don’t scale
Synchrony with Agile / DevSecOps action team

- We join head-to-tail; achieving STC requires contributions from two disciplines:

  \[ STC = \text{Rapid Acquisition Strategies} + \text{Rapid Capability Delivery} \]

- Outcome: New capabilities on contract fast + delivered fast. Therefore:
  - Contracting approach needs to be compatible with DevOps dev / delivery approach, and
  - DevOps dev / delivery needs to properly align with contractual expectations/requirements.

Summary Observations

- This is a giant Lean Six Sigma problem: increase throughput, increase predictability, minimize variability
- Constraint: Requirements variability and evolution over shorter time cycles complicate the problem
- Shared services and segmented acquisitions reduce timelines at cost of increased integration complexity
- PREDICTABILITY is valued by government and industry alike
  - Acquisition timing
  - Procurement content
  - Clearances
  - OCI rules
  - Cost evaluation methods
Questions & Concepts

Questions to Address:
• How to enable / motivate STC
• How to pay for STC
• How to measure STC

Ideas
Two categories (consistent with the STC metrics model):
• Requirement to Award
• Award-to-First Capability
Next Steps

1. Consolidate observations / ideas into a few simple messages

2. Identify specific examples to cite. Need IAWG help.

3. Guide a program through STC metrics

WE NEED EXAMPLES!
Programs familiar to GED to cite as examples of STC done right (or wrong). See Nick’s data call.
Some Ideas

- Shorter time from RFI to award due to clearer solicitation documents, resulting in less Q&A back-and-forth between bidders and government
- Outcome-based contract that emphasizes speed and functionality without directing implementation (e.g., SOO vice SOW)
- Payments based on development velocity
- Incentivize risk taking and fast failure on SMALL THINGS to LEARN FAST
- Concept of Minimal Viable Product as a strategy to increase speed of delivery to the warfighter based on the user's highest needs
- Use of innovation CLINs to help program pivot if needed
- Involve COR and security teams in solicitation creation (e.g., right-size the compliance clauses)
- Contract structure that allows changes in flight
- Start small, be iterative, and build on success – or terminate quickly
- Separate the development of mission-level software from development of IA-accredited platforms (i.e., what is developed on that platform is automatically accredited)
- AO sits with the program for a week, watches how they build software, and as long as we build software using an IaaS, deploy it on an accredited PaaS, and incorporate a modern CI/CD pipeline, it gets a continuous ATO.
Government Perspective
Co-Chairs: Establish recurring engagement at GED “QUINT SPO” meeting

Agile & DevOps Action Team Part 2: Form & Kickoff

- Talent: Provide GED leadership with “DevOps Starter Kit” info for clearance sponsorship and IR&D instances on C2S/S2P

- IAWG data call: examples of AF/IF criteria that created dis-incentives

- FGA: Identify options for providing industry-wide feedback on FGA architecture in format more useful and open than RFIs
  - Get membership access to FGA 2025 architecture (government stated it was ‘released’)
  - Consider Action team and/or RID to engage

- STC: Engage GED Contracts regarding “Contracting Performance” aspects and how industry would propose assessing them. What metrics?

- Potential Action Teams:
  - FGA Integration Model & Cross-Segment/Cross-Program DevOps
  - STC or new team address Waterfall TTO to DevOps Continuous Delivery & Integration
Open Dialog

Additional Topics for Consideration
Actions & Next Steps
No-Host Social
NRO IAWG Contact Information

- Nick Buck: nick@buckgroup.net  (703) 801-3405
- Ann Waynik: Ann.Waynik@tenica.biz  (571)-376-5641
- Mike Moran: mmoran07@peraton.com  (571) 524-1184

USGIF coordination:
- Shai Sobrino: shai.sobrino@usgif.org  (571) 392-7205
BACKUP
### Speed to Capability
Observations & Ideas

**Goal:** increase throughput, decrease acquisition variances

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Acquisition/RFP</th>
<th>Contracting</th>
<th>Development &amp; Tech Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>“Requirements Lock”</strong></td>
<td><strong>“Solicitation Bloat”</strong></td>
<td><strong>No Contracting Metrics</strong></td>
<td><strong>Waterfall Culture</strong></td>
</tr>
<tr>
<td><strong>Observation</strong></td>
<td><strong>Observation</strong></td>
<td><strong>Observation</strong></td>
<td><strong>Observation</strong></td>
</tr>
<tr>
<td>- Inhibits ability for programs to weave in new capabilities</td>
<td>- Drives away qualified performers, creates extra work – on both sides – without necessarily providing benefit</td>
<td>- Lack of specific, shared objectives for improving contract(ing) performance. Lack of concrete actions means status quo wins</td>
<td>- Inconsistent capability delivery chain and clunky transition to operations</td>
</tr>
<tr>
<td><strong>Contributing Factor</strong></td>
<td><strong>Contributing Factor</strong></td>
<td><strong>Contributing Factor</strong></td>
<td><strong>Contributing Factor</strong></td>
</tr>
<tr>
<td>- SOWs that “bake out” innovation or don’t articulate means to innovate (e.g., need to use study CLIN)</td>
<td>- Path of least resistance and lowest risk: “Include everything”</td>
<td>- Dearth of metrics for assessing quality of docs, RFPs, and contracting timelines</td>
<td>- Inertia within current hybrid infrastructure and lack of end user involvement</td>
</tr>
<tr>
<td><strong>Ideas</strong></td>
<td><strong>Ideas</strong></td>
<td><strong>Idea</strong></td>
<td><strong>Idea</strong></td>
</tr>
<tr>
<td>- Dynamic Reqs Management</td>
<td>- Right-size compliance documentation to effort size</td>
<td>- Measure against STC metrics based on industry standards and tailored to program profiles. [See template]</td>
<td>- Create nexus where technologist, operator/analyst, MSI, and acquirer can ID and advance solutions immediately, then document “requirements”</td>
</tr>
<tr>
<td>- Involve end users up front to define the “what” not the “how”</td>
<td>- Involve security teams in the solicitation creation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Expand use of IDIQs</td>
<td>- More two-way exchanges</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### STC Metrics – Template

**Presumed:** STC is inversely proportional to program size

There might be other relevant categories besides size (e.g., environment – legacy, modern, hybrid).

**Time-Based Metrics**

Plot each program’s Actual performance relative to its defined Threshold / Objective

#### SPEED TO CAPABILITY

<table>
<thead>
<tr>
<th>Capability</th>
<th>Requirement-to-Award</th>
<th>Award-to-First-Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actual</td>
<td>Threshold</td>
</tr>
<tr>
<td>Size</td>
<td>Program</td>
<td></td>
</tr>
<tr>
<td>$$$</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>$$$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>$</td>
<td>a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f</td>
<td></td>
</tr>
<tr>
<td></td>
<td>g</td>
<td></td>
</tr>
<tr>
<td></td>
<td>h</td>
<td></td>
</tr>
</tbody>
</table>

**IAWG might offer an industry benchmark for the class of capability category**

**Track actual performance against pre-determined threshold and objective specific to that program**

**1st graphic represents Requirement-to-Award (aka government)**

**2nd represents Award-to-First-Capability (aka industry)**
While DevSecOps in principle is technology agnostic, a number of modern technologies have emerged that can be enablers to make agility and devsecops easier to adopt. To be clear, the principles of DevSecOps and agility are independent of specific technologies and any team can adopt the principles and goals of rapid delivery of secure and reliable software. There are several technologies we consider enablers:

- **Cloud** - Cloud technologies enable rapid deployment and scaling of infrastructure as needed.

- **Containerization** - Containers abstract the underlying hardware and operating system, making it easy to have resilient environments.

- **Container Management/Orchestration** - Container Management / Orchestration makes it easy to deploy, monitor, scale, and manage the infrastructure of multiple containers which support a given system.
Key Enabler of Agile DevSecOps: Automation

- **Build and Integration** - Streamlining the tasks of building, compiling and assembling source code and related libraries into a working application.
- **Testing** - Enable repeatable, accurate, and reliable testing of application functionality to ensure that application quality standards are maintained.
- **Security Scanning** - Evaluate source code, infrastructure, and running applications to identify potential security vulnerabilities.
- **Configuration** - Defining the application configuration as a consistent and repeatable set of steps, reducing the risk of manual errors which can introduce performance and/or security issues.
- **Deployment** - Enable dynamic and parallelized deployment of applications to support incremental roll outs, feature flags, and other techniques to manage the deployment process and mitigate risks.
From Waterfall to DevSecOps
DevOps Challenges for Leadership

• Leadership can enable the adoption of DevSecOps by bringing its ENTIRE stack as a platform and by leveraging DevSecOps solutions.

• It is imperative not to “select” a limited option of tools. The key of microservices and containers is to be able to use the best solution to achieve the outcome desired. We should not limit options to the extend possible.

• Need to establish baseline requirements / thresholds for cybersecurity, test coverage, test results, documentation. This shouldn’t be reinvented per office but global to DoD as a standard practice to facilitate adoption.

• Once those baseline requirements are set, OCIO can provide CI/CD Platform’ stack with embedded security as a side-car container and provide pre-ATOs for systems using the Platform stack and automatically integrating the OCIO security baseline requirements.

• Bringing the entire stack as a Platform as a Service is key to avoid that each office reinvents the wheel and builds their own baseline requirements.

• Understand that Failing is a GOOD thing! It is part of learning. It allows us to understand what works and what doesn’t - AS LONG AS we leverage rapid prototyping, which allows for QUICK failure and mostly painless. It also allows us to reprioritize rapidly and leverage learnings.
DevOps Challenges for Acquisition Office

- DevOps is a complete disruption of the traditional Acquisition model. We need to leverage Sec 873/874 of the 2018 NDAA (check out https://cdnapisec.kaltura.com/index.php/extwidget/preview/partner_id/2203981/uiconf_id/38241181/entry_id/1_gib6brbc/embed/dynamic).
- No more complex RFPs with long planning phases with deliverables and milestones and fixed budgets. Keep in mind that when we write RFPs, we assume we know what we need and know exactly what the solution is. This doesn’t allow for us to learn and adopt new ideas along the way. This is the main cause of current failures. The world/ technology evolves, what we know evolves... We must be able to adapt continuously to guarantee success.
- This is NOT scope creep but proper agile scope management.
- RFPs should NOT define precise requirements with pre-defined technologies but focus on establishing mission outcomes and precise metrics to prove success of those end-goals.
- There is no “beginning” or “end” of a project, the project will continuously evolve based on mission needs. Yes, a project might be terminated but the idea is continuous evolution and development.
- The traditional accounting methods - where you have the R&D, development and deployment in production followed by maintenance/support phases - don’t apply anymore. We CONTINUOUSLY develop, deploy and learn. There are multiple releases per day.
- New procurement tools must enable continuous development and incentivize the use of containers, microservices and Agile methods.
- Most of the DevOps tools are opensource and the only costs are Cloud hosting/computing/storage. Some members are worried about costs of licenses and think about consolidation for cost saving - this is a non-issue. We pay for what we use as a IaaS/PaaS/SaaS model.
Legacy to DevSecOps => Strangler Pattern

• Martin Fowler describes the Strangler Application:
  • One of the natural wonders of this area are the huge strangler vines. They seed in the upper branches of a fig tree and gradually work their way down the tree until they root in the soil. Over many years they grow into fantastic and beautiful shapes, meanwhile strangling and killing the tree that was their host.

• To get there, the following steps were followed:
  • First, add a proxy, which sits between the legacy application and the user. Initially, this proxy doesn’t do anything but pass all traffic, unmodified, to the application.
  • Then, add new service (with its own database(s) and other supporting infrastructure) and link it to the proxy. Implement the first new page in this service. Then allow the proxy to serve traffic to that page (see below).
  • Add more pages, more functionality and potentially more services. Open up the proxy to the new pages and services. Repeat until all required functionality is handled by the new stack.
  • The monolith no longer serves traffic and can be switched off.

• Learn more:
2019 Agile & DevSecOps Action Team

Seth Wambold (Action Team Lead)

Focus Topic 1: “Terminology Gaps/Terms of Reference”
  Matt Reider (Topic Team Lead)
  Jay Eward, Ken Laskey, Rob Manogue, John Farrell, Scott Lawler

Focus Topic 2: “Scaling Agile & DevSecOps across GED Programs”
  Marc Kriz (Topic Team Lead)
  Joel Doyle, Sam Stollar, Eric Amberge, Pete Epstein, Shawn Lucas, Themba Hinke

Work Schedule:
• 3/26-4/12: Focus teams kickoff and pull together first thoughts on their topic
• Week of 4/12: Full team discuss first thoughts from Focus teams
• 4/23: Full team brief IAWG working session on observations, ideas, reccos
• Repeat to closure, move to next Focus Topic