Where Our National Security Begins...
Agenda

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

Events

- USGIF Working Group Summit: 27 August
- GED Agile Industry Day: TBD September
- GEOINTegration Summit: 27-28 September (Attracting Talent team)

USGIF request to shift NRO IAWG meeting day…which week?

Joint Action Team with NGA WG: Addressing TTO challenges
NRO IAWG
Action Teams & Topics

- 7/30/19 Agile & DevSecOps Team QUINT SPO Engagement
  - Terms of Reference
  - Speed to Capability
  - Scaling DevSecOps Across Programs
NRO
Industry Advisory Working Group

Agile & DevSecOps 2019 Team

Terms of Reference Focus Group

Matt Reider (Team Lead)
Ken Laskey        Jay Eward        Scott Lawler
Rob Manogue      John Farrell
Agile & DevSecOps 2019
Terms of Reference Focus Group

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

Approach
1. Identify commonly used agile process terms across GED and NRO
2. Identify terms that have divergent or misunderstood definitions
3. ID major commercial and agile government sources of definitions to create matrix
4. Coordinate common definitions with GED Chief Architect to ensure alignment
5. Highlight definitions or parts of definitions that enhance common understanding

Deliverable
A document containing standard Terms of Reference and their sources in order to align government and industry on a single set of definitions.

https://docs.google.com/spreadsheets/d/1njrGMElw7wXsRtu7kZtx1w-WWI_aJMhA9aIJaA1ZBg/edit?usp=sharing

DevSecOps Terms of Reference to be addressed in 2020
NRO IAWG
Agile Terms of Reference & Sources

Agile Process Terms (subset)
- Sprint
- Release
- User Story
- Story Point
- ScrumMaster
- Backlog Refinement
- Test Driven Development
- Scrum
- Scrum Meeting
- Sprint Review
- Sprint Demo
- Sprint Planning
- Product Backlog
- Behavior Driven Development
- Product Owner
- Product Manager
- Minimum Viable Product
- Velocity
- Definition of Done
- Sprint Retrospective

Selected Definition Sources
- Scaled Agile Framework for the enterprise (SAFe)
- Agile Alliance “Agile Glossary”
- SmartSheet “Ultimate Agile Dictionary”
- TechTarget “WhatIs” Glossary
- 18F Agile Lexicon
- The DevOps Handbook

IAWG & GED Chief Architect consensus: use SAFe definitions (when available) as common lexicon across government, industry, and vendors.
Alignment Process

Per GED recco, if SAFe glossary had a definition, that becomes the IAWG recommendation

If SAFe does not define, IAWG and GED representatives discuss & select recommended
Terms of Reference
Next Steps

- Provide inputs to GED Process Guide
- Incorporate QUINT SPO comments
- USGIF-wide peer review: broaden industry input
- DevSecOps ToR (future Focus Group)
Action Team: Speed to Capability (STC)

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

QUINT SPO briefing
30 July 2019
Speed to Capability Team: Purpose

Our Task
- Identify process, development, and programmatic sources of delay to delivery of capabilities
- Make recommendations for concrete action
- Questions to address re STC:
  - How to enable / motivate it?
  - How to pay for it?
  - How to measure it?

Current Landscape
- Delivered products can be too late to be relevant or don’t satisfy end user needs
- Ineffective processes & incentives for prime contractors to realize faster delivery cycles
- Complex acquisitions, coupled with risk aversion and preference for status quo, result in expensive, lengthy, ECP-driven programs
- Skills gap in acquisition workforce caused by increasing complexity of acquisitions in areas like IT; challenge increases with AI/ML

Desired Outcomes
- Accelerate time to get new capabilities on contract, and then…
- Accelerate delivery and approval of relevant, performant systems
Speed to Capability in Agile:
High-Level Observations & Ideas

• Program success is driven by the government and industry relationship beginning in acquisition and continuing through delivery and operations

• **Predictability** is beneficial to both government and industry, for example:
  • acquisition timelines;
  • OCI rules;
  • cost evaluation methods;
  • development locations (low to high)

• This is a big Lean Six Sigma problem: how to increase throughput, increase predictability, minimize variability

• Challenges:
  o Requirements variability and evolution over shorter time cycles complicate the problem
  o Shared services and segmented acquisitions reduce timelines but increase integration complexity

"Top 4" Ideas

1. Outcome-Based Contracts
2. Pre-Award Communications
3. Right-Sized RFPs
4. Development & Tech Transfer

Over 35 ideas harvested from across IAWG membership
Observation
Requirements “lock-in” inhibits ability for programs to weave in new capabilities

Contributing Factors
- Static requirements force solutions to be compliant and score well vice outside-the-box thinking
- SOWs that “bake out” innovation or don’t articulate means to innovate
- Change processes biased toward the status quo

Ideas
- Define the why, what, and who for…..but don’t dictate the how.
- Create contract structure (e.g., CLINs for innovation) to allow program to pivot in flight
- Incentivize risk-taking and fast failure on small things (e.g., MVP). Start small, iterate, learn fast, and build on success – or terminate quickly.
  - “How” options:
    o SOO vice SOW; Government buys X number of sprints; User stories vice requirements
    o More IDIQs to facilitate innovative industry base – broad scope, pools, periodic on-ramping and off-ramping
- Define/track value and performance metrics that resonate with mission owners and acquisition officials
  o Value can vary by customer based on need for speed, quality, productivity, or more.
  o Defining value as “user satisfaction” enables useful adaptations, with work tied to end user priorities
  o Industry-standard metrics: deployment frequency, change-failure rate, mean lead time, mean time to recover
Pre-Award Communications
Better communications pre-award: open and iterative, with the right people involved

Observation
Unclear expectations lead to guesswork by industry and thus harder time delivering what government needs
Risk aversion and inertia have led to a victory for the status quo

Contributing Factors
• Fear of tainting the procurement process
• Those who will ultimately be affected by the work are left out of planning phases
• Interactions at Industry Days often yield little useful insight

Ideas
• Applies to industry↔government communication but also within government. For example:
  o Involve multiple stakeholders to collaborate up front in solicitation creation
    ▪ Benefits: Government asks for right thing, industry better understands govt intent, industry prepares better proposals and solution hits mark. Ensures relevancy and enhances uptake/adoption. Helps to right-size the compliance documentation.
• Need ample opps for govt-industry communications and iterative feedback (e.g., developers, operations, security). Need to vet industry ideas and get feedback within proprietary environment, multiple times, well in advance of Draft RFP.
• More two-way exchanges. Allowed by FAR§15.201 but eschewed by many acquisition officials and lawyers, except in large “Industry Day” forums (where vendors won’t talk about their IP).
Right-Sized RFPs

Observations
• “Solicitation Bloat” deprives govt of qualified, innovative performers (mostly SBs), creates extra work – on both sides – without necessarily providing benefit
• Increasing complexity of acquisitions in areas like IT has caused a skills gap in the acquisition workforce

Contributing Factors
• “Include Everything” has historically been the path of least resistance and lowest risk re compliance
• High variance and low predictability of acquisition timing

Ideas
• Avoid complex RFPs with long planning phases which include deliverables and milestones and fixed budgets, and which can stifle ability to learn and adopt new ideas along the way.
• Right-size compliance documentation (especially docs listed as “reference,” which can be misleading, overly onerous, or unnecessary) to match the work being procured.
• Train program officers and contract managers to specialize in IT acquisition (e.g., mimic Digital IT Acquisition Professionals Program).
• Train people from a variety of functions (tech, finance, contracting, security) on Lean-Agile practices.
• Minimize CDRLs to the extent practical in order to avoid unnecessary effort and disrupting flow of execution
  o Start with minimum (e.g., financial CDRLs required by law) and add more only if deemed mission-essential
  o Make CDRLs “contractor format” to mitigate agile development issues tied to delivering classic CDRLs
  o Question for QUINT SPO: What should be a CDRL?
Development & Tech Transfer

Observation
Inconsistent capability deliveries and clunky transition to operations

Contributing Factors
Inertia within the current hybrid infrastructure and lack of end user involvement

Ideas
• Need mechanism for technologist (industry), operator/analyst (govt), integrator (MSI contractor), and acquirer (SPO/FFRDC/SETA) to identify and advance solutions – seize on immediate opps then document “requirements” thereafter
• Establish the enterprise dev/ops environment – even just a starting point – common to all ops sites upon which mission apps can be conceived, built, tested, deployed….and scaled rapidly
• Identify an unbiased entity (“Capability MSI”), whose sole job (and incentive) is to run that environment and move high-quality solutions (not their own!) into operational environments
• Enable development on unclassified network and transfer capabilities to classified network
• Use managed services (e.g., provisioning, shared libraries / resources, access to expertise)
• Seek Software OEMs committed to user adoption, not just selling tools, after licenses are bought
• Involve end users and product owners more deeply in agile development process (e.g., sprints) in order to fine-tune requirements and tailor system being developed.
Discussion and Next Steps

- Feedback Welcome:
  - Relevance to GED
  - Likelihood of having a significant positive impact on STC
    - GED interest in Public-Private partnership

- What additional topics are of interest?
- Recommendations for GED QUINT SPO vs Broader NRO?
- What messages to take back to industry?
NRO
Industry Advisory Working Group

Agile & DevSecOps

Scaling DevSecOps across Programs

Marc Kriz (Team Lead)

Shawn Lucas

Pete Epstein

Eric Amberge

Themba Hinke

Kevin Chasse

John Jeremiah

Sam Stollar

Joel Doyle
Scaling Agile & DevSecOps: Task & Deliverable

Best Practices & Industry Observations Survey/Report
Available at www.USGIF.org soon

1. Introduction
2. Aspects of DevSecOps and their definitions
3. Key Enablers of Agile DevSecOps
4. Alignment with GED practices
5. Scaling Agile & DevSecOps Across Programs
6. Constituencies - who/what group in GED will be affected?
7. Final Thoughts
8. Summary
Scaling Agile and DevSecOps across Programs

Enablers

- Willingness to consider working differently - “digitally dissolving silo’s”
- Senior leadership AND middle management top cover for change
- Technology that enables all team members to be on the same page, with collaboration, visibility and metrics crossing all boundaries.
- Management from across the teams (Industry and Government program to program) that agree on a common set of mission goals and outcomes.

Alignment is not a point in time…on-going dialog is essential
Scaling Agile and DevSecOps
Best Practices

■ Within Programs, Across Projects:
  o Run a Proof of Concept (POC), similar to an Open Source Software Project in order to generate base knowledge & experience
  o Pick a significant, meaningful project that incorporates multiple teams, across segments or mission enclaves

■ Across Programs:
  o Use technologies that enable DevSecOps automation; standardize approach
  o Agree on workflows, expected outputs, and hand offs between teams. (see COSS business model for examples: https://www.sciencedirect.com/science/article/abs/pii/S0950584918301277)
  o Measure teams on results & contributions to the whole,
  o Provide incentives and recognition for those whose velocity (code contributions), moves the mission or core project forward faster.

Cycle time compression may be the most underestimated force in determining winners & losers in tech. - Marc Andreesen
Scaling Agile & DevSecOps
Up Coming Topicals

- Best Practice: Architecture “Runway” to pace technology ahead of developers and communicate platform capability to the ecosystem
- Connecting Enterprise Portfolio Priorities to Program release priorities
- Agile Governance procedures
NRO
Industry Advisory Working Group

Look Ahead & Next Steps Dialog

CAPT Nick Buck, USN (Ret)
Ann Waynik
NRO IAWG QUINT SPO
Look Ahead

- Monthly Working Sessions 4th (5th) Tuesdays: All are welcome!
- Scaling Agile Team scheduling August QUINT
- Terms of Reference: send to broad Industry review
- Attracting Talent team ready for government engagement
- PROPOSED Action Team: Accelerating Transition to Operations
“S2P Corner”

Latest & Greatest…

Topics & Issues Discussion

Explore on CWAN/JWICS @ https://jportal.S2P.proj.nro.ic.gov
(U) GED's Requirements Flow Taxonomy

**SRs**

**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**

Graphic is UNCLASSIFIED
Kanban steps:

**Step 1**: Visualize your work. First, break down the flow of work from the moment you start it to when it's finished into distinctive steps and draw a column for each. ...

**Step 2**: Limit work in progress. ...

**Step 3**: Don't push too hard. …. Pull

**Step 4**: Use, monitor, adapt and improve
“C2S Corner”

Latest & Greatest…

Topics & Issues Discussion
NRO IAWG
Action Teams & Topics

- *Hybrid Cloud Business Model*
- *Previous data call*
  - Unintended consequences of AF/IF
  - Industry feedback on FGA architecture
Agile & DevSecOps 2019
Focus Area Topics

- Agile Terms of Reference
- Scaling Agile and DevSecOps across GED Program Offices
- Contracting strategies, structures, and incentives
- DevSecOps Terms of Reference
- Training gaps, standardization, and program-specific implementations
- ROI expectations and perceptions
- E2E Mission Thread Closure in an Agile & DevSecOps world
NRO IAWG Action Team

Hybrid Cloud Action Team

Chris Arroyo (Team Lead)

Al Stewart  Robert Shelton  Keith Barber  Tim Stewart
Hybrid Cloud Action Team

What are we trying to accomplish?

Problem Statement

As the next generation of C2S, C2E will present the NRO with an opportunity to leverage a cloud agnostic environment with multiple options. Without a good understanding of how to adopt cloud agnostic model that works for NRO, the agency runs the risk of not realizing all the potential benefits. Failure to fully understand all the challenges involved and lacking a strategy for adoption will put the mission unnecessarily at risk. Additionally, lack of clarity and understanding from the government will inhibit industry's ability to meet the needs of the customer.
Create a recommended framework to consider the impact of various cloud adoption scenarios on the NRO - including decision authority, business model impacts, and exit criteria.
As NIST defines “cloud” as: “…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
## NIST Cloud Deployment Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Cloud Infrastructure Is</th>
<th>Managed by</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud</td>
<td>Provisioned for exclusive use by a single organization comprising multiple consumers (for example, business units, etc.).</td>
<td>Owned, managed, and operated by the organization.</td>
<td>On or Off premises</td>
</tr>
<tr>
<td>Community cloud</td>
<td>Provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).</td>
<td>May be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination.</td>
<td>On or Off Premises</td>
</tr>
<tr>
<td>Public cloud</td>
<td>Provisioned for open use by the general public.</td>
<td>Owned, managed, and operated by a business, academic, or government organization, or a combined organization.</td>
<td>On the premises of the cloud provider.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.</td>
<td>Each infrastructure may be owned, managed, and operated by one or more of the organizations involved.</td>
<td>On or Off Premises</td>
</tr>
</tbody>
</table>
Identify Approach - Cloud Model

Implications

• **Increased flexibility** - Competition is a *good* thing and GED can leverage this for increased savings.

• **Sunk Costs** - have you broken down the cost to migrate to the cloud and factored in investments already made?
  
  • Implication is that it may not be cheaper to move to the cloud

• **Attracting the right talent** - *Cleared* Cloud expertise can be difficult to recruit

• **Data and Operational Complexity** - Multiple clouds increase the management complexity

• **Ownership** - Is there a clear understand on who owns what?
Decision Authority

• Whether it’s GED leadership or program managers, everyone with a stake in the process should be involved.

• Data to be considered should be gathered through the following:
  • Cost benefit analysis
  • Comparative performance analysis
  • Metrics established for expected performance advantages.

• It is important to thoroughly consider pros and cons in each option before deciding to migrate to the cloud.

Source: General Services Administration
Sample Decision Tree

Sample Decision flow for migrating or hosting USG Information Technology systems in the Cloud

1. Determine Reasons for migrating
   - Reduction in Hosting Costs
   - Improving System Performance
   - Improving Security
   - Publicly accessible data
   - CIO Mandate
   - Consolidate multiple locations
   - Other

   Cost Benefit Analysis completed
   Comparative Performance Analysis completed & Metrics established
   FedRAMP, DoD SRG or other Security, PIA, PII requirements
   Technical requirements completed
   Acquisition Analysis completed
   Business Case Analysis completed
   Contingencies Analysis completed

Cloud hosting
CSP Evaluator, SI, Broker or CSP

Decision Point
Existing Hosting Facility

Source: General Services Administration
Framework - Business Model Impact

• **Different models will have different impacts** - Mission needs will direct GED to different models

• **Conduct a Pilot** - Use a subset (approximately 5%) of locations or users that are a close representation of the whole, to conduct a pilot. The purpose of the pilot is to determine the following
  - Anticipated costs
  - Capacity/resource usage
  - Services needed to support the cloud
  - Acquisition contract type needed

• **Different Models = Different Costs** - Build a business case based on a clear understanding of the costs around:
  - Data Migration
  - Integration and Testing
  - Consultants

Source: General Services Administration
Framework - Business Model Impact

• **Determine Model for Mission Need** - This should be based on a clear understanding of the operational needs, mission, and security requirements.
  
  • Below is an image from NOAA that can be used as a guide:

Framework - Exit Plan

- **Risk Management** - Identify, in writing, a plan for addressing risk across the directorate, acquisition, security, etc.

- **Address Exit Plan EARLY** - Clearly understand from both government and industry what and who needs to be involved when leaving your cloud service provider
  
  - Clearly understand ownership rights for data and applications

- **Develop a clear SOP document** - should accomplish the following:
  
  - Roles of the CSP, Federal government and any other interdependent Subject Matter Experts
  
  - Continuous monitoring related to Security & Vulnerability analysis
  
  - Actions to conduct (and responsible Point-Of-Contact (PoC)) during a security incident
  
  - Regularly test the SOP’s and update with current PoC information details as needed.

Fundamental misunderstandings of Agile with an award fee based program will drive Agile anti-patterns onto the program. For example:

- Customers changed. New Customers didn’t understand agile development & changed approach
- Team was castigated for not focusing on requirements instead of grooming backlog, velocity, etc.
- Fee negatively impacted, Senior levels of customer didn’t accept reclama.
- Unintended consequence: disenfranchised development team, resulting in retention issues.

Standardization: Differing perceptions on what constitutes a “Good” Award Fee

- Government COR “does not believe in 100%” and “80% a good score.”
- Some programs start at 100% and work down, others start at 80% and go up from there.
- Unintended consequence: government may be happy with prime but PM is still fired.

Don’t presume business implications of the incentive structure are understood.

- Industry doesn’t communicate implications that well either –
- BD folks that attend the meetings are NOT the line-of-business PMs that have to deliver
- Govt should require that any industry interaction include at least one mid/senior LOB person
Data Call #2: Capturing Industry Feedback on FGA while maintaining level playing field

- Quarterly dialogues (like the December industry day)
  - discuss current status, feedback received, and their reaction to that feedback.
  - Follow up each session with one-on-ones.
  - Requires customer commitment and time, but could create a stronger industry partnership

- Host Open Industry Roundtable discussions in addition to forums like Industry Days
  - Organize participation into relevant groups, e.g. NRO IAWG
  - Direct discussion, trade show attendance, peer networking groups, etc.

- Go beyond RFIs with small group discussions.
  - Near unanimous feedback that paper RFIs are of low value and ROI given the time required.
  - Trust relationships are needed so those sharing feel that their IP (best practices) is protected.
  - Idea: GED send delegations to trade shows and set up separate meetings with various vendors. Gather best practices from as many different vendors as possible. Prepare specific asks beforehand. Empower government staff that it is permissible to meet with commercial vendors and follow up after.

- Resurrect the $50K-$100K Study Task approach used in SIGINT post-HASA/LISA timeframe
IDEA for Data Call #2: Capturing Industry Feedback on FGA while maintaining level playing field

Concept: Annual “Market Surveillance & Research” Cycle

- **Step 1:** “FGA 2025 Communication Day”
  - Govt explain the program and allow for initial Q&A during the session (ala 2016 GED Industry Day).
  - Govt ID’s specific questions they would like addressed by industry during the day.

- **Step 2:** 60 minute “Market Surveillance” dialogs with industry over a 2 month period
  - Industry provide perspectives for FGA2025 and address govt questions from Day 1.
  - Includes both technical and business areas.
  - Format: Two-way conversation. Not an uber-structured, constrained meeting where govt are not allowed to speak. Govt PMs/engineers/operators sharing what they really are trying to achieve, what bugs them, what architectural characteristics are of significant value to them, and what key EXTERNAL interfaces are challenging them.
  - The content of these sessions would NOT be available beyond the govt and specific company.

- **Step 3:** “FGA 2025 Communication Day 2”
  - Reflect govt architectural adjustments in light of the industry engagement.

- **Step 4:** 30 minute, focused “Market research” meetings on specific topics
Government Perspective
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
Action Tracker (needs updating)

- **STC**: Engage GED Contracts regarding “Contracting Performance” aspects and how industry would propose assessing them. What metrics?
- **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
- **Talent**: Provide GED leadership with “DevOps Starter Kit” info for clearance sponsorship and IR&D instances on C2S/S2P
- **New Action Team (Joint w/NGA WG)**: Waterfall TTO to DevOps “incremental”