Where Our National Security Begins...
Agenda

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

Follow ups

• NRO Cloud Day: 3/6/2019
• IC ServiceNow Users Group
• QUINT SPO debrief and future schedule
IAWG: Nick Buck, Seth Wambold, Ann Waynik, Ken Laskey, Joe Chioda

QUINT SPO Questions/Inputs

– Can industry provide some examples of where award fee language created unintended disincentives? (Pat Brennan, CA)

– Does implementation of DevSecOps across segments require a certain architecture? Does degree of coupling between Framework and Services matter? (Charlie Meadows, GG SPO)

– Should DevSecOps be implemented in pieces of programs (micro) or the overall program (macro)? Does it make a difference to adoption? (Zach Cole, CA)

– Does DevSecOps change methodologies behind Independent Cost Estimates, e.g. the cost estimating parameters? (Brian Schmanske, I2 SPO)

– The topic multi-segment scale out, to include cross-program dependency tracking across multiple DevSecOps efforts is of interest to all of the SPOs.

General Observations

– QUINT SPO open to IAWG returning on a regular basis!

ACTION: IAWG Data Call. Industry examples of AF/IF criteria that created unintentional consequences and/or disincentives
“C2S Corner”

Latest & Greatest…

Topics & Issues Discussion
“S2P Corner”

Latest & Greatest…

Topics & Issues Discussion

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

• Attracting Talent
• Agile & DevSecOps 2019
NRO
Industry Advisory Working Group

Attracting Talent Action Team
Update & Forward Planning
GOVERNMENT “Attract” the Talent

- Consider a portfolio approach to Contract Types (IDIQ vs Single Award)
  - Balance flexibility and speed of IDIQ TO approach with continuity and base of Single Awards
  - Investigate relationship between size/segmentation and contracting strategy impact on industry base

- Focus on Price/Performance and Cost Realism over Labor & Wrap Rates
  - Recognize that Talent drives fully-burdened and direct labor costs
  - Higher quality, faster delivery is less expensive and more predictable over course of program

- Emphasize Deliverable- or Milestone-Performance Based Contracts vs LOE
  - Provides Government leverage; provides Contractor flexibility to deliver talent
  - Buy “Capabilities” instead of Candidate Resumes
  - Reward risk taking (Innovation is typically risked up in proposals)

- Security Waivers, Continuous Evaluation or Interim Security Clearances
  - Provide Additional Security Billets to each Company and Interim Clearances
INDUSTRY: “Retain” the Talent

- Meet Needs
  - Sign-on Bonus, Retention Bonuses, Pay off School Loan
  - Quicker Promotions, More Career Flexibility

- Provide Continuing Training
  - Agile Processes/MBSE, Renewal of Certificates, Latest Seminars/Conferences
  - Provide “RIDE ALONG” Mentors

- Provide Corporate and Program IRADs
  - Accept Risk with Performance-Based Deliverable Contracts
  - Be More Creative with Cost/Schedule/Performance Constraints
  - Look at Functional versus Technical experience (to broaden talent pool)
  - Similar Pay Scales for those with “Functional” Experience

BOTTOM LINE

GOVERNMENT’S ROLE: Attract the Talent

INDUSTRY’S ROLE: Train & Retain the Talent
NRO
Industry Advisory Working Group

Agile & DevSecOps Action Team 2019
Kickoff Update
Agile & DevSecOps Focus Topics

1. Must address terminology gaps: Terms of Reference
   - Contractor and tool agnostic language
   - Focus on industry standards and norms

2. Scaling Agile and DevOps across GED Program Offices
   - Challenge: how to implement DevOps with cross-program dependencies?
   - Challenge: Release prioritization across projects and programs?
   - Does implementation of DevSecOps across segments require a certain architecture? Does degree of coupling between Framework and Services matter? (Charlie Meadows, GG SPO)
   - Multi-segment scale out, to include cross-program dependency tracking across multiple DevSecOps efforts is of interest to all of the SPOs.
   - Should DevSecOps be implemented in pieces of programs (micro) or the overall program (macro)? Does it make a difference to adoption? (Zach Cole, CA)
Additional DevSecOps Focus Topics

3. Contracting strategies, structures, and language
   - Differences of opinion on CP/AF/IF (deliverable) vs FFPLOE (story point)
   - Traditional CDRL-based approaches must evolve to accommodate DevOps
   - Can industry provide some examples of where award fee language created unintended disincentives? (Pat Brennan, CA)
   - Does DevSecOps change methodologies behind Independent Cost Estimates, e.g. the cost estimating parameters? (Brian Schmanske, I2 SPO)

4. Training gaps, standardization, and program-specific implementations
   - Who is training the government, FFRDC, and SETA?
   - Engineering Practice Managers, Thread leads, and Product Owner roles

5. Address ROI expectations and perceptions: what you get out vs what you put in on Agile & DevSecOps

6. E2E System Closure in an Agile & DevOps world
   - Impact of Continuous Delivery & Integration models on TTO, FOSS/COTS approval as multiple locations, etc
   - “Iron Bar of Enterprise Test”: Mission Partner + NRO Ground Segments + Space Segment
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
DoD Enterprise DevSecOps Platform
(Software Factory)
DAU Presentation

DRAFT v1.3 – UNCLASSIFIED – PRE-DECISIONAL
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:
NRO
Industry Advisory Working Group

Accelerating Speed to Capability:
Topic Plan & Ties to Agile & DevOps team(s)
### 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).

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>

Time-Based Metrics

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

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

1st graphic represents Requirement-to-Award (aka government)
2nd represents Award-to-First-Capability (aka industry)

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

Government Performance

Industry Performance
Government Perspective
Action Tracker

- 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
Common Theme: Accelerating Speed to Capability across Programs
Observations on Agile & DevOps:
- It is a culture shock to developers, program managers, SED, and MOD
- It has great promise but faces major culture, training, and business process obstacles

Questions:
- Is DevOps fundamental to NRO cloud adoption and Future Ground Architecture?
- How does DevOps impact/change the NRO Operating & Business Models?
- What Contracting approaches are optimal for Agile & DevOps?
**“DevOps” vs “Agile”: Working Definition**

**DevOps (clipped compound of “development” and “operations”)**

- Culture & Practice emphasizing collaboration and communication between stakeholders, including consumers, developers, operators, and testers, to improve software delivery and infrastructure changes.
- A convergence of culture, process and automation/tools to achieve faster delivery of robust, correct features in small batches from idea to operations.

*Customer Need* → **Scaled Agile** → **Lean-Agile** → **DevOps** → **Continuous VALUE Delivery**

- **Scaled Agile** describes what is needed
- **Lean-Agile** describes the minimum viable product & how to build it
- **How do we deliver value faster to the customer? “DevOps”**
Agile & DevOps are vital to realizing the NRO Future Ground Architecture vision
  – Quality + Resiliency + Data Centricity + Speed to Delivery cannot be met without it
  – Next generation of software developers will not know anything else
  – Uptake across Industry and Government reflects the maturity of Agile DevOps practices

Both NRO and NGA are demonstrating successful DevOps programs on contract
  – NRO S2P providing tooling needed to manage Agile / Dev Ops (eg. Jira, Confluence)
  – Both CP and FFPLOE approaches can work…AF and IF components are recommended
  – Emphasis on delivery vs FTE, Product Backlog prioritization, and incentivizing speed

GED Primes are implementing Agile & DevOps projects and see business benefits
  – DevOps being tried / deployed at factories – not yet mature – but lessons being learned quickly

Challenges:
  – Culture: must address process & vernacular conflict between Waterfall, Agile & DevOps
  – Operating Models: A&A and Transition to Operations are #1 and #2 process challenge areas
  – Contracting: approaches & language must evolve to harness power of Agile & DevOps
  – Legacy System Migration: Recognize & address challenge legacy install base presents
  – Training: Government CO, PM, COTR, and Engineer training & certification is essential
  – Software Procurement: Supply Chain must evolve to support DevOps timelines
2018 Agile & DevOps Team Observations: Scaling out Agile & DevOps Demands Culture Change

- **Shift from Waterfall to Agile & DevOps** changes the NRO operating model
  - Transition to Ops & NSIS delivery models are contrary to Continuous Deployment
  - Waterfall requirements definition & decomposition impose “batch constraints” on velocity

- **Shift requires culture change and real-time collaboration between:**
  - Acquisition
  - Program Management
  - Developers
  - Infrastructure Providers (NISP)
  - Software Service Provider (NASP)
  - Security
  - Operations

- **Leadership Commitment to Changing Culture**
  - Must take place at the Director level and include all echelons
  - Recognize conflict between Waterfall & Agile/DevOps approaches
  - There is a mission opportunity cost to delay. Ensure MOD, Security, and SED share in **desire and accountability** to accelerate speed to operations.
  - Accept a learning component: effectiveness evolves, it’s not pre-designed

*Waterfall process “culture” constrains speed to mission available in Agile & DevOps*
2018 Agile & DevOps Team Observations: Contracting Challenges & Questions

Key Considerations in Agile & DevOps contract implementation
- Active management of staffing mix
- Government partner...no playing “gotcha” on speed #s.
- Govt must focus on product roadmap & priority. Govt MUST own the priorities
- Transparency of tools with criteria
- Regular engagement/rhythm with government, e.g. re-prioritization meetings
- Government discipline to NOT revert to LOE behavior by asking for people or FTE

Must Account for “SE” or “Support” functions (it’s not just scrum teams)

One size still doesn’t fit all: Deliverable based Solutions vs Labor Hour (CP v FFP LOE v FFP)

Government Observation: Government not trained or experienced in DevOps contracting

Industry Observation: Contracts language, Award Fee approaches can dis-incentivize

Question: How do you pay for speed, independent of contract type?
- IDEA: Incentive fees for deliveries per unit time (sprint team velocity improvements)
- IDEA: Award fees for accurate estimation of velocity (story points) and delivery
2018 Agile & DevOps Team Observations: Must Address “Transition State” Between Legacy & New

Discussion: Should we combine modes for optimum benefit?
- DevOps mode can provide capabilities scheduled for waterfall delivery
- DevOps contributions to waterfall delivery can have benefits of small batch size
- Do not need Big Bang adoption of DevOps to start seeing DevOps value
- Recommend starting DevOps with small but significant project
  - Show value, Learn, grow
  - Needs to be a real program... “pilot” project should mean “first” not “trial”
- Migrate larger Waterfall development to appropriate mix with DevOps

Challenges:
- DevOps delivery speed can overwhelm Waterfall transition processes
- Waterfall time spans drive backlog in DevOps resulting in schedule and cost escalation
- Waterfall governance models tend toward “one size fits all”
2019 Agile & DevSecOps Action Team
Topical Areas for Discussion

**Area 1: Culture**
- Terminology & Vernacular to foster common understanding & manage conflict
- Evolving (and new) government/industry roles and accountabilities
- Legacy migration to DevOps and relation to Current/Future DevOps programs
- Manage perceptions & expectations: How do you measure ROI of DevOps?

**Area 2: Program Management & Business processes**
- ATO Automation & Continuous Delivery impact to A&A, TTO, NSIS, Op Tempo
- Multi-segment scale out including dependency management & cross-program vs program-specific
- Topic: Incentivizing on “delivered velocity” and accurate estimation of story points in bids?
- Topic: Set CAIV/Price to which bidders respond with how much requirement they can meet?

**Area 3: Contracting for Agile & DevOps programs**
- Acquisition / requirements / contract approaches (e.g. SOO vs SOW, CPAF/IF vs FFPLOE vs FFP/IF)
- Procuring “story points” as a measure of development capacity and velocity.
- Assessing realism based on demonstrated velocity and P/P on relevant developments
- How much should the government specify vis a vis DevOps implementation?
Area 4?: Cyber Security for Agile & DevOps programs...DevSecOps

- Security Requirements must be agreed upon by government early in process (STOP if they are not nailed down)
- Integrate security and A&A processes as a flow to continually work down risk but maintain development pace
- Add risk-based management decisions to A&A process to provide an accurate snapshot with workoff plans and verification closing open issues over time
- Consider automated security control verification to speed up the DevSecOps process and add integrity for informed AO risk decisions
- Leverage control inheritance to cover most controls in the cloud infrastructure reducing the burden on individual applications and systems where possible
- Provide inheritable enterprise security services to support and accelerate application and system deployment
GED scaling Agile and DevOps across Program Offices
- Challenge: how to implement DevOps with cross-program dependencies
- Challenge: Release prioritization across projects and programs

Training gaps, standardization, and program-specific implementations
- Who is training the government, FFRDC, and SETA?
- Engineering Practice Managers, Thread leads, and Product Owner roles

Must address terminology gaps: Terms of Reference

Address expectations and perceptions of what you get out vs what you put in on Agile & DevOps

Contracting strategies, structures, and language
- Differences of opinion on CP/AF/IF (deliverable) vs FFPLOE (story point)
- Traditional CDRL-based approaches must evolve to accommodate DevOps

E2E System Closure in an Agile & DevOps world
- Impact of Continuous Delivery & Integration models on TTO
- “Iron Bar of Enterprise Test”: Mission Partner + NRO Ground Segments + Space Segment

Does the current plan capture everything?