Where Our National Security Begins...
NRO
Application Service Provider
Industry Advisory Working Group

Working Session
October 3, 2017
Agenda

- Welcome & Introductions
- Government Perspective*
- “Snapshots”
- “S2P Corner” & “C2S Corner”
- Action team discussions
- No-Host Social
Government Perspective
Snapshots

- State of GEOINT inputs
- DevOps Starter Kit
- GED Leadership engagement
- FGA Industry Day
“S2P Corner”

Latest & Greatest...Fact vs Fiction

Topics & Issues Discussion

CWAN accessible @ HTTPS://S2P.proj.nro.ic.gov

Unclassified S2P JPortal @ https://www.s2p.cloud
S2P Release 2.1 Platform Day:
NASP Strategic Objectives

• Software Supply Chain
  – Leverage technologies such as Sonatype & Ion Channel (CaseGuard) to streamline the customer software supply chain process

• ATO Automation
  – Leverage technologies such as SonarQube, Fortify, Sonatype, Security Center to automate the *re-accreditation* of a system

• Multi-Domain DevOps Pipeline
  – Leverage cross-domain solution (AWS Diode?) to provide automated movement of software artifacts from low to high

• Data Services & Innovation Environment
  – Integration of data services and Innovation environment into S2P baseline
Release Update

S2P Release 2.1 Included

- JIRA Data Center
- Confluence Data Center
- TestRail
- API Gateway (WS02) enhancements
- Hardened Windows AMI
- ServiceNow
- Selenium GRID (brokered by DIA)
- JPortal enhancements

S2P Release 2.2 Objectives

- Transition of Innovation Environment
- Creation of Data Services Environment
- Initial stand-up of S2P FVEY
- OpenShift Container Platform (OCP)
- Jenkins 2.x
- Hardened RedHat AMI
“C2S Corner”

Check out: Bi-Weekly C2S Community Forum

re:Invent Conference 11/27-12/1
NRO IAWG
2017 Action Teams & Topics

*DevOps Team Business Model Dialog*
DevOps Action Team

Jay Eward (Team Lead)
Clark van Buskirk
Ken Laskey
Jared Putman

Pete Epstein
Shawn Lucas
Suzanne Sincavage

John Farrell
Andy Murren
Jeff York

Observations:
• DevOps is a culture shock to developers and programs
• DevOps has great promise but faces major obstacles

Questions:
• Is DevOps fundamental to cloud adoption by NRO?
• How does DevOps impact the NRO Operating Model?
• Does DevOps change the NRO business model?
DevOps OR Waterfall?

“Bimodal IT”* - the practice of managing two separate but coherent styles of work

Mode 1 (Waterfall)
- Single sequential progression from requirements to development to test to deployment
  - Typically requires long timelines (e.g. years) from problem to delivered solution
  - Concentrates on development of many (possibly diverse) capabilities to be delivered at the same time (or as a small number of drops)
- Baseline for Government programs with which any other approach must likely combine and coordinate

Mode 2 (DevOps)
- Evolving requirements prioritized as backlog
- Multiple cycles (e.g. sprints) to develop, test, and deploy additional capability as capability becomes available
  - More frequent delivery of more focused capability
  - Delivery of small batches, fully tested and avoiding accumulation of issues that harder to isolate in larger batches
- Goal is rapid delivery of value to stakeholders
- Numerous methodologies, e.g. Agile Scrum, SAFe

* Source: Gartner
DevOps AND Waterfall Hybrid

- Recognizes transition state between legacy system development and emerging framework and services development
- Combines 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 governance models tend toward “one size fits all”
DevOps Culture Change Impact to NRO Business Model

- Redefine what is meant by requirements
  - User feedback validates or corrects what has been built (delivered outcomes)
  - Requirements are really a collection of agreements over course of development
  - How to we measure this as progress?

- Evolution of Contracting approaches to account for DevOps
  - Outcome based contracting
    - Deliver desired solution, not list of CLINs
  - Incentivize collaboration and timely, accurate, secure delivery
  - Incentivize risk taking and fast failure on way to success
  - Payments based on development velocity
    - Developer/PM/AO bid and assign points for sprint
    - Developer is paid on delivery and commitment accuracy
    - Identify and encourage stretch goals

- Periodically schedule sprint to burn off prioritized technical debt
Contracting for DevOps

- Challenge 1: Government not trained or experienced in DevOps contracting
- Challenge 2: Contracts language, Award Fee approaches can dis-incentivize
- Requirement: Deliverable based Solutions vs Labor Hour FTE
- “Time boxing”: schedule and resource loading as independent variables
  - Sprints and Epics are fixed duration (i.e. schedule is fixed)
  - Resources over a fixed duration are known
  - Capability delivered is dependent variable…how far down the priority list did you get?
  - Success based on a ratio: maximizing innovation or capability delivered “per” dollar
- How do you pay for speed?
  - Incentivizing sprint team velocity improvements?
  - Incentivizing accurate estimation of velocity (story points) and delivery?
- Accounting for Development vs “Support”
  - Engineering/Development = Scrum Teams
  - Support = CM, CDRL management, Security etc
- IDEA: Re-introduce Cost as an Independent Variable (Govt states price)
Question: Is Industry Adopting DevOps as its Preferred Approach? Or is it Resisting?

- **Challenge:** anecdotal evidence from a few government programs
  - Is industry adopting DevOps on its own or waiting for government direction?
  - Minimal lessons learned and information flow between industry and government.

- **IDEA:** “crowd source” or “survey” the industry base for…
  - Government programs where DevOps is used
  - industry partner use (DevOps vs Waterfall) mix.

- **Suggestions for information to gather would start with:**
  - name of project
  - sponsoring organization
  - who doing the hands on work
  - what capabilities have they demonstrated
  - planned next steps
  - eventual goals
Questions for Industry

- What is the business impact?
  - ATO automation
  - Continuous delivery
  - Multi-Domain DevOps

- What is industry assessment of S2P completeness?
- How do you measure ROI of DevOps?
- What should government specify ref DevOps implementation?
NRO IAWG
2017 Action Teams & Topics
COTS vs GOTS Make-Buy Trades
COTS-GOTS Make-Buy: Factors to Consider

OPERATING MODEL FACTORS

- Acquisition Strategy
  - ABC (Adopt, Buy, Create) vs CBA?
  - “Speed to Need” (Day 1 vs Year 1 capability)
  - Incremental & Agile approaches (esp. COTS)

- Ease of development with Service contracts
  - Measures of Success
  - QA/QC Independent
  - Ownership – Make/Buy/Integrate components

- Procurement Factors
  - Complexity of NDI Product procurement
  - Different pots of money: Dev vs O&M?
  - Licensing (OSS contribution?/Middleware)
  - Warranties, Indemnification, Cyber liability

BUSINESS MODEL FACTORS

- Technology cycle compression
- Funding models (government & industry)
- Services vs. Licenses:
  - Obs & expenditures (Govt)
  - Revenue recognition (Industry)
- TCO (Govt) and Cost recovery (Industry)
- Intellectual property influences
- Maintenance and licensing, royalties
- Protections and indemnification
- Retirement and refresh
- Risk models

ARCHITECTURAL FACTORS

- Open Architecture
  - Level of componentization
  - Degree of API publication
  - Open I/Fs vs Open Source code

- Requirements
  - 80-90% fit vs 100% fit vs not avail in marketplace
  - Outcome based vs Activity based
  - Tech Readiness/Product Maturity
# Risk Comparison – COTS/GOTS/Hybrid Models

*Is Hybrid the “Best of Both Worlds”?*

<table>
<thead>
<tr>
<th>RISK AREA</th>
<th>COTS</th>
<th>GOTS</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>• Developed in anticipation of market need</td>
<td>• Requirements must be well defined upfront to control risk.</td>
<td>• Lowest baseline risk. Development risk focused on extending COTS with new GOTS functionality.</td>
</tr>
<tr>
<td></td>
<td>• Purpose built, custom coding.</td>
<td>• Purpose built, custom coding.</td>
<td></td>
</tr>
<tr>
<td>Integration</td>
<td>• Dependent on API availability</td>
<td>• Purpose built integration</td>
<td>• COTS integration points allow use as open platform</td>
</tr>
<tr>
<td></td>
<td>• May require wrapping</td>
<td>• Code can be modified if req’d</td>
<td>• Minimize custom integration</td>
</tr>
<tr>
<td></td>
<td>• Legacy system complexity</td>
<td>• External Interface complexity</td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td>• Market driven performance</td>
<td>• Requirements driven testing and performance. “Have it your way.”</td>
<td>• Requirements driven performance &amp; testing PLUS widely available components</td>
</tr>
<tr>
<td></td>
<td>• Unique mission configuration or adaption to legacy may be required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>• Cost amortized over larger expected market.</td>
<td>• Labor throughout lifecycle. Cost from requirements, testing and service rates.</td>
<td>• Minimize direct labor TCO.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Leverage available COTS</td>
</tr>
<tr>
<td>Schedule</td>
<td>• Available off the shelf with min modification. May require labor to configure or adapt.</td>
<td>• Minimum 6 months to capability. Timeline driven by requirements, testing and available services.</td>
<td>• “Day 1” capability + Requirements, testing and available services driven</td>
</tr>
<tr>
<td>Maintenance</td>
<td>• Services and version control per licensing parameters.</td>
<td>• Maintenance services. Version Control and promotion to operations.</td>
<td>• GOTS &amp; COTS delineated terms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sustaining outage</td>
<td>• Managed via maintenance model</td>
</tr>
<tr>
<td>Security</td>
<td>• Indemnification, warranties, IA risks/costs carried by supplier.</td>
<td>• Supports unique security needs.</td>
<td>• Indemnifications and protections, w/support to unique security needs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requires labor to maintain.</td>
<td></td>
</tr>
</tbody>
</table>
Potential COTS-GOTS Procurement Models

**COTS**
- Govt buys 100% functionality, but it addresses less than 100% of reqts
- Govt request new requirement
- Vendor assesses market ROI and pays to develop “100%” solution, OR Govt defers requirement and waits for Vendor roadmap

**“Accelerated” COTS**
- Govt buys 100% functionality, but it addresses less than 100% of reqts
- Govt identifies “delta” requirements
- If no COTS Market ROI, Govt pays vendor for accelerating capability
- If potential Market ROI, Govt/Vendor cost share accelerating capability

**COTS-GOTS “Hybrid”**
- Govt buys COTS but it meets less than 100% of requirement
- Govt assigns “delta” reqts to integrator
- Integrator extends COTS via API/SDK

**GOTS**
- Govt builds 100%
- Govt assigns reqts to integrator
- Govt self-indemnifies & ensures compliance with Economies Act
- Vendor-free supply chain

Assumptions: both COTS/GOTS providers use open source
Open Dialog

Additional Topics for Consideration

Actions & Next Steps

No-Host Social
IAWG Contact Info & Additional Information

- Nick Buck: nick@buckgroup.net  (703) 801-3405

- Co-Chair Position vacant: consider volunteering!

- Justin Franz (USGIF coord): justin.franz@usgif.org (571) 392-7205
# NASP IAWG Progress

## Addressing Business Model Obstacles to Cloud Adoption

### Are We There Yet?

<table>
<thead>
<tr>
<th>ISP-ASP Adoption Challenge Area</th>
<th>IAWG Action Teams</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ - Acquisition processes&lt;br&gt;  - Tech cycles shorter than acq cycles&lt;br&gt;  - Market research &amp; tech currency gaps</td>
<td>✓ Incentivizing govt/industry behavior&lt;br&gt;  ❖ Requirements: Over-ask and Under-Ask&lt;br&gt;  ☐ Cloud business/revenue models</td>
</tr>
<tr>
<td>✓ - Procurement Models (“ABC” vs “CBA”)&lt;br&gt;  - Perceived bias against paid licensing&lt;br&gt;  - Role of OSS misunderstood&lt;br&gt;  - Contracts: S/W vs Services</td>
<td>✓ Pay-for-Use Licensing &amp; ELA models&lt;br&gt;  ✓ GOTS/COTS/OSS Business models&lt;br&gt;  ❖ Software Business 101 course</td>
</tr>
<tr>
<td>✓ - Integration Models&lt;br&gt;  - Segmentation &amp; OCI concerns&lt;br&gt;  - Integration vs Configuration&lt;br&gt;  - Waterfall vs Agile DevOps</td>
<td>✓ FGA Framework segmentation &amp; OCI&lt;br&gt;  ✓ Software Development vs Integration&lt;br&gt;  ❖ Adoption of Agile &amp; DevOps&lt;br&gt;  ❖ Systems Integration vs Software Integration</td>
</tr>
</tbody>
</table>
What is an IAG?

Industry partners self-organizing to discuss matters of mutual concern and provide pragmatic recommendations regarding the industrial base.

An IAG is:
- Volunteer-based
- Strategic in nature
- Objective (pros & cons)
- Open to participation
- Company-agnostic
- Problem-centric
- Focused on outcomes

An IAG is not:
- Sponsored by the government
- Restricted in participation
- Proprietary
- A pursuit/capture venue
- A shaping & positioning opportunity
- A venue to recommend products
- An open ended discussion forum

Future Business Models are of Strategic Importance to the Industry Base
NASP IAWG: Charter & Objectives

Mission: Help NRO ASP and Industry jointly achieve transformation objectives
- Identify business models that will support government and industry objectives
- Identify potential pitfalls and recommend potential solutions

Charter: Provide expert industry resource and sounding board focused on:
- Business aspects of emerging acquisition models used to acquire software services
- Ramifications of componentizing software applications,
- Benefits accrued to the government & industry,
- Intended and unintended consequences against the industry base,
- Limitations and viability as a reasonable course of action

Objectives:
- Provide strategic industry input to a changing acquisition landscape
- Provide an objective and neutral venue for discussing approaches to business models
- Foster effective communication between government and industry leadership
Guiding Principles & Deliverables

- **Provide Options, not “answers”**
  - Emphasize trade space and alternatives, not defining or recommending “the answer”:
  - Provide feedback (sometimes confidential) and socialize concepts in a trusted-partner venue

- **Constrain the problem set: Step 1 for Action Teams is defining the deliverable**
  - Emphasize speed and pragmatism over exhaustive research and perfect world scenarios
  - Quick hitting analyses, “Magic-Quadrant”-like outputs, roundtable
  - Timely enough to make the dialog relevant in the issue du jour

- **Remain credible**
  - Discussions must be vendor, supplier, and integrator agnostic, not just by product/company, but by architecture as well. Must self-police to ensure objectivity.
  - Recommendations must be realistic
  - Sweet spot is the bridge between policy and execution

- **Establish a functioning & robust Industry – NASP leadership interface**
  - Know when to defer to other groups or venues
  - Be responsive and objective above all
  - Open and collaborative (not duplicative of other efforts, involve as necessary)