Where Our National Security Begins...
Agenda

- Welcome & Introductions
- “Snapshots”
- Action Team Updates & Discussions
  - System Level Integration & TTO
  - Hybrid Cloud Adoption & Business Model
- S2P Data Call
- Government Perspective (as applicable)
- Open Dialog
“Snapshots”

USGIF Programs Team Update
June 2020
“Snapshots”

SED “Enterprise Commercial Consortium”

Upcoming Events of Interest

- COVID business rhythm impacts update

NAWG Action Team efforts

1. Impact of OCI Policy on Acquisition (Bob Whiteman)
2. Improving Software Acquisition (Colin Thomas)
3. System Level Integration, Accelerating TTO (Joint w/ NRO IAWG)
NRO
Industry Advisory Working Group

Accelerating System-Level Integration & Transition to Operations (TTO)

Action Team
Sub Team Topics to assess

- Integration – No single organization tasked with Ground integration
  - Pros and Cons to Top-Down Integration Approach
  - Pros and Cons to Diversified Integration Approach
  - What is the level of integration responsibility between Govt and Industry
- How does the Government Incentivize to deliver fast
  - Industry incentives to deliver
  - Government incentives and processes to accept CI/CD
- How to Sync CI/CD between NRO and NGA
  - What is the baseline “as is” at NRO vs NGA; the “ideal”? 
  - ID philosophical differences to CI/CD approaches to TTO (risk tolerance differences)
- Thoughts on how MOD can participate in CI/CD
  - How to deliver assured mission. How much risk is too much?
  - What about risk of delay?
Joint NAWG-NIAWG Discussion: System Integration & TTO

- Government line of effort: **Blueprint for Lean Governance**
  - Focus is Agile Governance
  - Culture change across MOD/SED and Acquisition Directorates
  - NRO Instructions to be tailored accordingly

- IAWG opportunity: Transition Section review & comment
  - MOD lead author
  - Key need: agreement on what defines “ops relevant” vs “no impact” changes
  - Consideration: must incorporate perspectives from across stakeholders
  - Would benefit from industry perspectives, best practices, and peer review

- Emerging issue topics:
  - Requirements development skillsets
  - Requirements stability and evolution in SAFe enterprises
  - End user engagement approaches to realize Agile potential

**Call for Volunteers: Blueprint review (Transition Section)**
NRO Industry Advisory Working Group

Chris Arroyo, Matt Madigan, Matt Manning, Renard Paulin, Steve Sharp, Steve Thomas

TTO Subgroup 3: Synching CI/CD Between NGA/NRO

June 11th, 2020
Objectives for Month of June

• Compile your list of questions for the Government and the organization or organizations you believe is the target audience
• Compile your list of questions to ask the USGIF Industry membership to gain insight into your topic
Questions for Government

• What is the timeline the NRO would like to have DevSecOps available/implemented?
• Is the government planning to include DevSecOps requirements within current or future contracts?
• Is the intention to eventually have all development efforts, regardless of size or scope, use government provided DevSecOps environment. If not, what type of program, effort or requirement would not use the government's DevSecOps environment?
• Is the government's intention to have their DevSecOps environment completely in the cloud or would any on premise datacenter DevSecOps resources be stood up. If so, which ones?
• Would the government have any interest in Industry provided/owned DevSecOps capabilities, environments or software factories?
• What tools, services, functions are the government's highest priority within the DevSecOps pipeline?
• How does the government foresee it will continually update the tools, services, and processes within it DevSecOps environment to keep pace with developer needs and technology advancements
Questions for Government (cont)

- Will a single organization/office within the agency control/manage the DevSecOps pipeline/environment while all other organizations/office utilize the services?
- Does the government differentiate between development, release, and deployment processes?
- Are there organizations that the government looks to as a model for implementing DevSecOps?
- Does the government have a standardized way to define a “release candidate”?
- What components go into an ideal release candidate?
- Does the government define release management as its own discipline?
- Is the government interested in hybrid or best of breed solutions between COTS, GOTS and Open Source and how does the government see this functioning in a DevSecOps environment?
Questions for USGIF Members

- Do you currently have or are you developing your own DevSecOps environment, capabilities or software factories?
- Do you currently employ DevOps developers/engineers or have DevOps LCATs?
- What do you consider the greatest benefit of using DevSecOps pipeline/process?
- What do you consider the worst part of using DevSecOps pipeline/process?
- Do you believe the government is misusing the DevSecOps pipeline in any way?
- What recommendation do you want to offer the government related to DevSecOps?
- Are there any requirements, contracts, scope, effort you would request the government not utilize DevSecOps to deliver?
- What do you need from government, in the context of guidance, that can optimize your software delivery process?
NRO
Industry Advisory Working Group
Data Call

S2P Future Investment
S2P Future Investment Data Call: Summary

- Total submissions: 21 total, most spanning all areas
- S2P evolution focus (summary captured)
  - a. needed functionality
  - b. automation to achieve speed to mission goals
  - c. platform stability and security
  - d. documentation, on boarding, and user training
- “Low-to-high” development focus (in-work)
  - a. tooling
  - b. CONOPS
  - c. Security
  - d. Cross-domain code migration

Reminder: this is an Industry-Driven Data Call, not a Government RFI!
S2P Evolution: Functionality

- Evolve into a PaaS with fully integrated CI/CD pipelines
  - Adopt end-to-end DevSecOps tool chains vs making devs create their own
  - Don’t offer tools, offer secure, high-availability pipeline(s) w/ integrated workflows
- Mature to Enterprise capability for ALL tools validated into S2P
  - Must go beyond MVP initial capabilities to scale as service provider
  - Labor-intensive workarounds for non-enterprise capabilities are wasteful
  - Each OSS tool with Enterprise capability should have a roadmap to it
- Release Orchestration
  - Integrate existing tools, teams, and processes to release S/W in a fast, secure, compliant and predictable way.
- Connectivity
  - Need documented, approved way to reach FVEY environments from NF dev boxes
S2P Evolution: Functionality

- **Database Vulnerability & Configuration Assessments**
  - If dB in dev are not protected they get to prod with vulnerabilities (COTS/FOSS alike)
  - Dev teams should run baseline assessments and establish practice of continuous assessment to ensure vulnerabilities are remediated prior to submitting application to RMF process.
  - Recurring dB scanning ensures compliance with continuous monitoring policies.

- **Software support**
  - Inclusion of APIs, SDKs and dev tools from COTS vendors to enhance and accelerate interoperability of NRO Data Services

- **Web Application Vulnerability Assessments**
  - Assess security of web applications accessing underlying dB systems.
  - Conduct dB credential assessments (least privilege model)
  - Adopt continuous assessment of privileges for users and NPEs.
S2P Evolution: Automation

- Fully embrace CI/CD but reduce tool chain complexity

- Many open source artifacts come in different packaging (RPM vs TAR vs DEB vs MSI) at different versions (10+) with different provenance.
  - Recco: Provide access to all artifacts for a given release instead of one specific artifact per request. This expands the number of users able to make use of the approved software and reduces amount of requests sent to S2P.
  - Recco: Identify official vendor artifacts with a badge, tag, or other mark to ensure users can easily find ones supported by that vendor.
  - Work together with vendors to enter new versions (which can contain security patches) into the approval pipeline so that users can gain access to them as soon as possible and to reduce the amount of requests sent to S2P: it’s a virtual certainty that there will be a request for every major, minor, and point release.
S2P Evolution: Automation

- **Granular ticketing system**
  - Shouldn’t need to use the “general question” at all
  - Responses to “general question” tickets should not take multiple days

- **Accelerate workflows by hosting data and data services that make data immediately exploitable without ETL from source to analyst desktop.**
  - Object identification
  - Automated categorization and availability
  - Location analytics and alerting

- **Provide centralized self-service dB security assessment**
  - Consider appliance-based self-service model allowing multiple dev teams to run automated self-service vulnerability scans against dB systems and front end connected web applications
  - Mandate API integration + self-serve ticketing systems for COTS/FOSS dB systems
Mission critical support
- Need Five 9’s available on-call support with response times
- Need HHH security rating
- Current issue: no dedicated help desk to call for emergency issues

Availability
- Take advantage of additional AWS regions coming online to create geographic separation to achieve higher availability and resiliency

Security Groups: S2P currently uses “general use” security groups
- Impact: with shared groups, any change from COMM or other efforts causes failures across environments.
- Recco: Provide ability to manage security groups tailored specifically to the application
- Recco: Provide infrastructure level security groups that contain the enterprise level tools and provide OS level security groups that can reach out externally to enterprise services such as NTP servers for time synchs
Devs forced to use pre-made IAM roles based on efforts and not use generic one that all have access to. (Need to debate/discuss)

Hardened Deployments
- Recco: capture and implement up-to-date security best practices for all components of the open source applications to help ensure users are hardening their deployments.

High Value Asset (data) dB security and assessment
- Ability to accept and execute multiple requests simultaneously as well as maintaining current builds and fixing scripts.

Configuration
- S2P OpenShift isn’t config’d to supply IP addresses to provisioned services; support applies NodePort, which is inflexible and fragile

Use of COTS tools that allow for warranties/proven results
S2P Evolution: Documentation, Onboarding, & User Training

- Need sufficient notifications and effective upgrade plans prior to major maintenance windows
  - Recco: Prior to any window an upgrade plan should be presented and approved by COTRs; review upgrade and deployment activities with efforts during Scrum of Scrums
  - Recco: Train infrastructure teams on system maintenance and upgrades

- Need info and documentation on what is needed across all S2P Fabrics
  - Recco: Create a community page for cross-collaboration (include workflows, Docs)
  - Recco: Update Confluence pages to provide easy to follow clear blueprint on how to go through the full S2P path to production, starting with OnBoarding

- Expand Vendor Documentation (both FOSS & COTS)
  - Work with vendor base to provide up-to-date documentation of all components on S2P.
  - Provide dev teams documentation and onboarding procedures on self-service ticket requests to orchestrate vulnerability scans and receive findings/remediations.

- User engagement: clear understanding of goals needed for users to perform their daily functions based on S2P.

- Need instructions on using the full tool chain to build confidence
  - Recco: if it’s available to the public it MUST be made available on high side developers
S2P “Low-to-high” Development: Tooling

- No effective Cloud Monitoring in place (i.e., Nagios, Zabbix, OP5) or User Attribution (lack of structured roles)

- AMI cloud images are not standardized or consistent across the different S2P environments. (S2P) Standardize AMIs; develop reoccurring plan to update AMI & cloud formation templates

- Increase the use of existing COTS tools that are available to the public and within the community. Enable a streamlined and repeatable testing/security protocol to keep near-equivalency in public (unclass) and IC systems.

- Tooling interoperability is absolutely key. Provide a robust diversity of tools available to developers to increase the attractiveness of the S2P platform and thus its adoption. Forcing developers to adopt tooling in the form of an all-in-one solution will achieve a desirable result. Developers resist change and anything NRO can do to allow developer flexibility will benefit end-user satisfaction.
  
  - As the diversity of tools grows, consider enterprise-grade tools that are supported by the OEM and have built-in functionality that makes them much easier to manage at scale.
Develop a “Use before Buy” mentality

Tooling to move code and dependencies from low to high should exist and be automated. We should follow the lead of other agencies that have the ability for developers to commit code into lowside repositories which are automatically synced (after being scanned) with highside equivalents that can then trigger CI/CD pipelines to build and test the changes.

FedRAMP has been successful developing a CONOPs for implementing security controls. S2P should learn from the FedRAMP CONOPs to improve consistency and ease of use.

The CONOPS needs to be standardized across the NRO and hopefully across the IC. There are different processes for different organizations.

Survey commercial industry to investigate new technologies to make this happen.
S2P “Low-to-high” Development : CONOPS 2

- Work with the government to provide an “Advanced Commercial Cross-Domain Development Facility” (AC2D2F). This would be a place for Agile Commercial SW Developers to execute ‘low-side’ SW development and then migrate that code ‘high-side’ and provide final test and demonstration capability from both domains. This facility would have both office space (unclassified and classified) as well as appropriately managed Cloud Service Provider access (multi-cloud) as well as Bare Metal Cloud configurations all in a SD-enabled development environment.

- By definition, this AC2D2F would have the following characteristics:
  - Configured for co-located classified and unclassified Office/Workstation space that is directly ‘wired’ into commercial/USG Networks and SW Development Cloud Infrastructure that is both classified and unclassified
  - Small, affordable office suites for individual SW Development companies
  - Expansive shared use space where TEAMS of developers can prototype/collaborate and do MASH-UPS on targeted USG identified ‘hard problems’.
  - Conference Rooms and USG Demonstration Stations – A place where applications developers can demonstrate solutions for USG sponsors/customers/end-users
  - Simultaneously provide private workspaces together with a shared, collaborative space in order to support company-to-company innovation.
  - Facilities Security Officer as a Service (FSOaaS) - An embedded FSO function that can work with commercial companies to facilitate all of the personal & facilities clearance issues.
Organizations should consider engaging security SME’s to conduct security assessments on how to securely deploy a low to high system to accommodate the increasing importance of remote telework.

- Consider prototyping ideas to implement newer commercial technologies in this area

Certs and Accreditation Access Consistency

Ease the process for vendors to get off-site secure access (CWAN)

Cloud Consistencies, Access, Accreditations across networks

Development teams need a modern software factory with a fully functional assembly line that is efficient, easy to manage, and able to quickly build, test, and deliver their applications. Governance policies and tests can be automated and then included in CI/CD build, test and deployment processes. With this approach, ATO approval timelines can be significantly reduced and is in line with soon-to-be-released streamlining from NIST for Automated Control-Based Assessments with Open Security Controls Assessment Language (OSCAL). This type of automation makes it possible to run automated ATO checks as frequently as every release. Best practice recommendations are:

- Provide a consistent toolchain across all environments
- Recognize that code + collaborative details together convey context across environments
- Establish automation via RESTful API
- Enable selective feedback from the High-side to the Low-side
S2P “Low-to-high” Development: Cross-Domain Code Migration

- S2P maintains an approved Software Catalog for the classified systems, because some contractors used unclassified environments. There should be a similar approved Software Catalog on the unclassified systems.

- Unclassified development can introduce security vulnerabilities and takes significant time to transfer into high side development impacting responsiveness to need. Invest to enable rapid unclassified Continuous Integration/Continuous Delivery (CI/CD) into the classified DevSecOps pipeline.

- Multi-Level Security (MLS) solution combined with data trust, secured through an immutable ledger securely, deploys compute and data resources to multiple domains/security levels from a single repository.

- Automated Cross-Domain Code Migration would make it easier to move SW code. In addition to moving from Low to High, it would be fantastic if we could move down from a higher to lower security level, preferably all the way to unclassified.

- Recco: Look at methods to better standardize the Low and high side development environments and automate the transfer of files up and down.
“Low-to-high” Development: Cross-Domain Code Migration

- The tools and APIs for finding approved software should be the same high and low. The approved software should be the same high and low. The dependency management tools and contents (Maven, Ruby Gems, PyPI, Docker registries, etc) should be the same. And the deployment approach should be the same: teams should not use technologies or services that are not available highside.

- Cross-domain code migration aka Failover Cluster Migration
  - Cross-domain secure file transfer technology
  - Failover Cluster Migration technology

- Process-as-code is useful here. With the right Release Orchestration tooling, all of the release process you define can be exported as code to your source control system – whichever one you choose. You’re then able to version the whole process of how to deliver that software, and store the process-as-code in your SCM tool. A typical use case for Process-as-Code is in air gap or cross-domain situations, where the next deployment destination is in the other room and there’s no connection between networks. In this case, you practice and validate the process on the low side. Then you sneaker-net the process (as code) into the other room, where you have a high-side environment running another instance. You scan it to make sure there’s nothing vulnerable, then migrate it in.
NRO
Industry Advisory Working Group
Hybrid Cloud Adoption & Business Model Action Team

Chris Arroyo  Romano Romani
Keith Barber  Al Stewart
John Farrell  Ron Alford
Scott Lawler  Marc Kriz
Tim Stewart  Michael Rudd
Hybrid Cloud Adoption & Business Model Action Team Charter & Overview

• Objectives:
  1. Build a *decision framework* to guide government/industry on path to hybrid cloud
  2. Characterize “as a Service” business and acquisition models
  3. Identify alternatives for deciding which cloud and how (centralized vs distributed decisions)

• Approach & Ground Rules
  • Unbiased, research-driven best-practice recommendations
  • We may NOT recommend virtues of one cloud over another!
  • Different agencies identify decision criteria levels based on own mission requirements

• Aspects to Consider:
  • Operating Models – who makes the decisions? At agency level or program by program?
  • Business Models- cost (i/o performance, data storage and compute) and data rights
  • Acquisition Models- [need to explore]
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: annmwaynik@gmail.com (571)-376-5641

USGIF coordination:
- Shannon McAvoy: shannon.mcavoy@usgif.org (703) 793-0109 ext 118