DevSecOps for Government

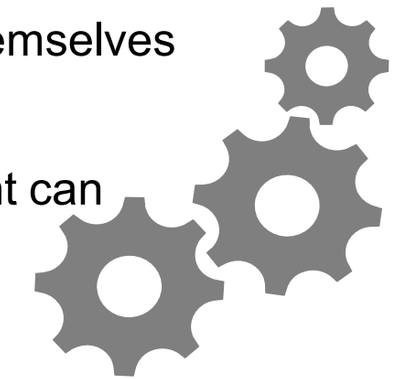
Is it really different?

Trac Bannon, Senior Principal
November 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Snowflakes or Sameness?

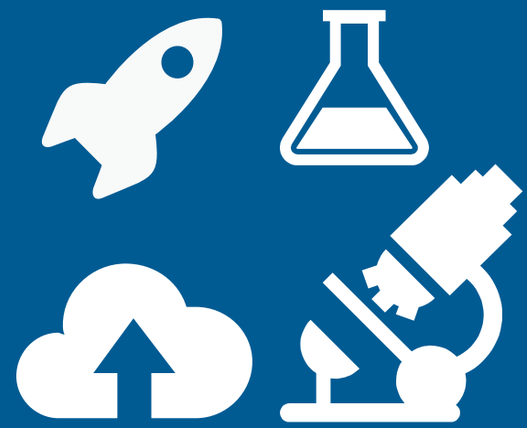
- Government agencies, services, ministries, and organizations have long considered themselves so unique they could not benefit from broader industry beyond specific technologies.
- While government leverages industry tech, there is growing recognition that government can learn from industry methodologies
- Government has typically been focused on oversight as opposed to design/build
- Tremendous energy to “do DevOps” without considering which aspects to adopt and the real challenges: talent , transformation, and transfer of risk.
- Both industry and government lack common definition of DevSecOps and exemplars
- Social tech media drive the hype that rapid building is the answer when the challenges faced by government are more complex



Understanding the differences, unique challenges, and context of public/defense sector DevSecOps will drive tailoring and problem solving needed to serve governments

MITRE

Sameness:
Thirst for Innovation



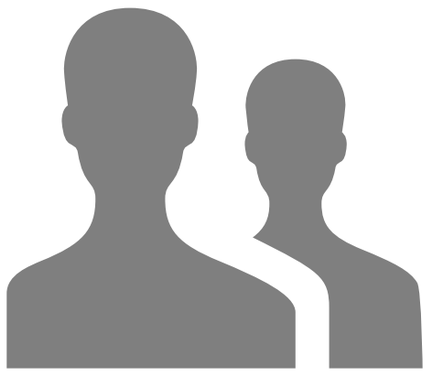
Snowflake: Problem Space

- Generally, government manages acquisition and focuses on oversight
- Much of the government software needs are for complex adaptive systems; these are system of systems with mission workflows involving hardware/software integration
- DevOps literature and use cases are often greenfield/cloud/app-focused
- Most of the software supports government workers, scientists, and warfighters
- Government info systems need to protect many types of data (classified, PII, HIPPA, financial)
- Cloud is not always an option; there is a need for completely isolated environments and data centers
- Some solutions must operate in austere environments (e.g. remote locations or after natural disasters, war)

Snowflake: Acquisition

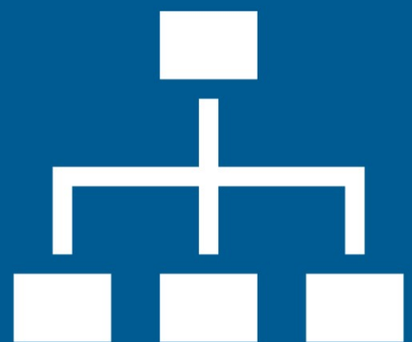
- Much, if not most, delivery of software for governments is contracted and acquired
- Government wants innovation but government acquisition smarts have not caught up yet
- New acquisition guidance is being piloted now such as Adaptive Acquisition Framework (AAF) though adoption is difficult
- Transformation for existing programs and portfolios often takes contract rework
- Defense, in particular, cannot transfer risk and must deal with it directly
- When acquisition is awarded, there are different teams or different contractors for each skill: architecture, development, testing, security, operations with varying goals and success criteria

Snowflake: Workforce

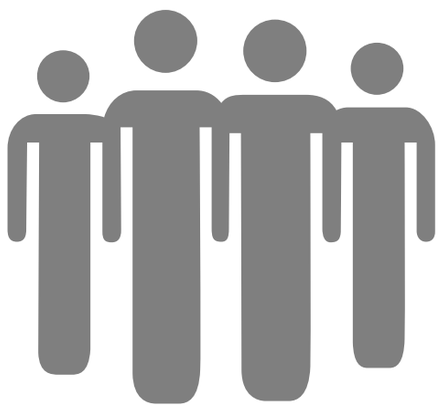


- Government staff often focused on oversight instead of implementation
- Govt staff are trained and operate in roles that are not as technical as their contractor counterparts
- Government suffers from an aging workforce with nearly 20 times as many IT employees over 50 as are under 30[a]
- The existing workforce needs to be retrained and provided with upskilling opportunities
- There is difficulty in direct hiring given wage and benefits offered by industry
- We are asking folks to be more directly involved—the shift is happening quickly without giving personnel an opportunity to become comfortable with the change
- While government may understand the need to change, it is difficult truly transform
- Government is just now learning to refocus on transformation instead of transition

Sameness:
Conway’s Law



Snowflake: Organizational Structure & Culture



- Cross functional teams generally do not exist
- Greenfield development is often assigned to the same waterfall or TOGAF/DODAF inspired team structures
- Different teams or different contractors are given responsibility to delivery skills institutionalizing “throwing over the wall”
- The cultural barriers introduced by traditional hierarchy, political appointments, service-member rotations are huge
- There is much less turnover in the work force; transformation demands new leaders and workers to infuse new mindsets
- The new state is radically different; transformation is difficult [b] especially it impacts people personally [c]
- Unionized IT shops need special consideration and negotiation
- A resulting trend is towards more centralization especially for DevSecOps

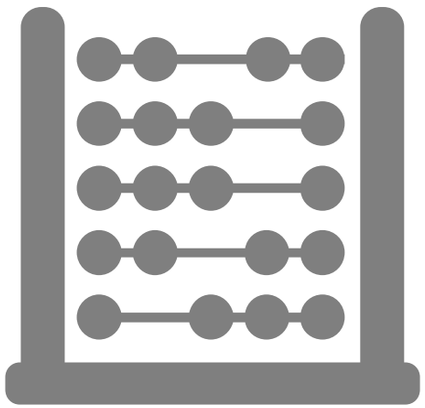
Snowflake:

Too much DEV / not enough OPS

- Developer-centricity abounds – factories and pipeline focus on developers getting code into production quickly
- New teams are created to “run DevOps”
- Software factory mentality awards pipeline implementation and pipeline usage to different contract for even a single system
- Looking for fast software development and not the feedback loop from operations
- Hyper CI/CD focused given the maturity of automated unit testing. The focus is on CI
- Agencies and organizations are often less involved in Ops so have less exposure and less understanding of the value
- The addition of Sec to Dev(Sec)Ops is helping to widen the aperture

Sameness:
Focus on Value

Snowflake: Defining Value



- Return on investment (ROI) does not hold relevance but senior government leaders want to hear about ROI.
- Determining value completely depends on the mission needs and services provided
- Civilian agencies more likely to have metrics and value based on services to citizens
- What about defense…?
- The govt acquisition community is not very good on identifying these type of measures and resulting metrics for determining the ROI of the chaining being instituted
- Being abstracted away from operations side of DevSecOps means being even more removed from determining value
- Concept of a single product owner who can prioritize the roadmap based on value generally cannot be achieved

Sameness:
Cyber vigilance

Snowflake: Pedigree, ATO, and more

- No room for error when the lives of citizens and sovereignty of a nation is at stake
- Increasing software footprint means increased cyber risk
- Authority to Operate (ATO) can take up to 18 months
- Open Source cannot simply be adopted without understanding the impact and intent of contributions
- Understanding software pedigree/lineage is paramount
- Industry/Government currently working on a software bill of materials (SBOM) standard to improve lineage reporting

Sameness:

Pride and Passion

MITRE

Tracy L. Bannon
TBannon@MITRE.org
TracyBannon@gmail.com
https://www.linkedin.com/in/tracylbannon
@TracyBannon

Special thanks for though contributions from Paul Vencill, Dr. Bob Cherinka, Carlos Vera, and MITRE Lab's software engineering division (L180).

Disclaimer: The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

References:

[a] FEDweek. “New Data Shows Aging Federal Workforce, Especially in IT.” *FEDweek*, 21 Aug. 2019, www.fedweek.com/fedweek/new-data-reinforce-concerns-about-aging-of-federal-workforce.

[b]“Leading Change: Why Transformation Efforts Fail.” *Harvard Business Review*, 13 July 2015, hbr.org/1995/05/leading-change-why-transformation-efforts-fail-2.

[c]“What Is Transformation, and Why Is It So Hard to Manage?” *Change Leader’s Network*, changeleadersnetwork.com/free-resources/what-is-transformation-and-why-is-it-so-hard-to-manage. Accessed 29 Nov. 2020.