

# DevSecOps for Government

*Is it really different?*



Trac Bannon, Senior Principal  
September 2021

**MITRE** | SOLVING PROBLEMS  
FOR A SAFER WORLD™

# Who am I?

Tracy L. Bannon

- ✓ Senior Principal with the MITRE Corporation
- ✓ Software Architect and Engineer
- ✓ Focused on problem solving using software



/trās/

# What are my tags?

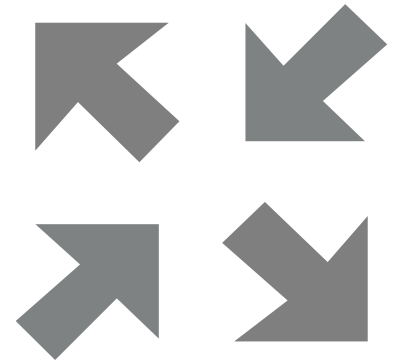




*Understanding the differences, unique challenges, and context of public/defense sector DevSecOps will drive tailoring and problem solving needed to serve government*

# Differences and Similarities

- Government leverages industry tech
- Growing recognition that **government can learn from industry methodologies**
- Government has typically been **focused on oversight**
- Tremendous energy to “do DevOps” instead of dealing with **real challenges**
- Industry and government **lack common definition** of DevSecOps and exemplars



# Similarity: Thirst for Innovation



# Difference: Problem Space



- Government **manages acquisition** and focuses on oversight
- DevOps literature are often **greenfield**, cloud, and app-focused
- Reality is often **brownfield on metal**
- Cloud is not always an option
- There is a need for **isolated environments** and data centers
- Some solutions must operate in austere environments (e.g. remote locations or after natural disasters, war)

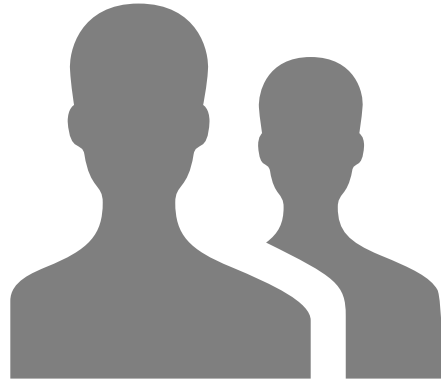
# Difference: Acquisition



- Most government **software is contracted** and acquired
- Government **acquisition smarts** have not caught up yet
- Different contracts for **different skills**
- Varying goals and success criteria
- Changes to existing efforts means **contract rework**
- New acquisition guidance is being piloted though adoption is difficult

# Difference:

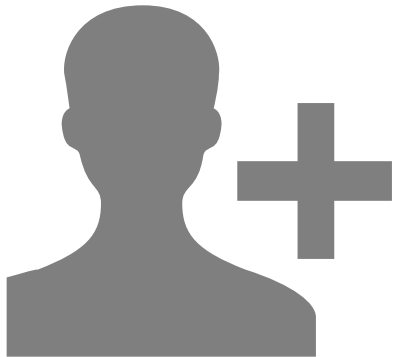
## Government Workforce



- Staff often focused on **oversight not implementation**
- Trained and operate in roles that are **not as technical as contractor counterparts**
- Government suffers from an **aging workforce** with nearly 20 times as many IT employees over 50 as are under 30<sup>a</sup>
- **Muscle memory is exceptionally strong**

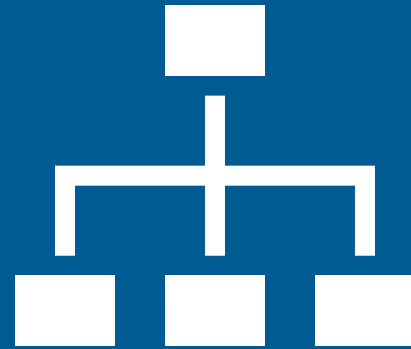


# Difference: Hiring & Retention

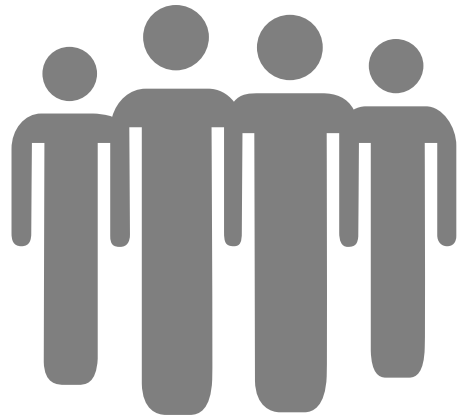


- There is **difficulty in direct hiring** given wage and benefits offered by industry
- Need to attract all levels especially **experienced architects** and engineers
- **Workforce needs to be retrained** and provided with upskilling opportunities
- Limited technical **career paths**

# Similarity: Conway's Law



# Difference: Organizational Structure



- **Cross functional teams** generally do not exist
- TOGAF/DODAF inspired team structures (waterfall, separation of architectures)
- Greenfield development is often assigned to **waterfall structured organizations**
- Institutionalized “**throwing over the wall**”
- **Unionized IT shops** need special consideration and negotiation

# Similarity: Centralizing Trend



# Difference: Culture



- The **cultural barriers** introduced by traditional hierarchy
- Political appointments **change funding**
- **Less turnover** in the work force
- **Service-member rotations** cause MTTC
- Transformation demands new leaders and workers to **infuse new mindsets**

**Similarity:  
Transformation is difficult<sup>b</sup>**



# Difference:

## Too much DEV / not enough OPS



- New groups are created to “run DevOps”
- **Developer-centricity** abounds
- Flawed use of **velocity as success marker**
- Quantity over quality
- Missing emphasis on **feedback loop** from operations and users
- Structure does not exist yet for Devs to have Ops responsibility

# Similarity: Metrics Madness

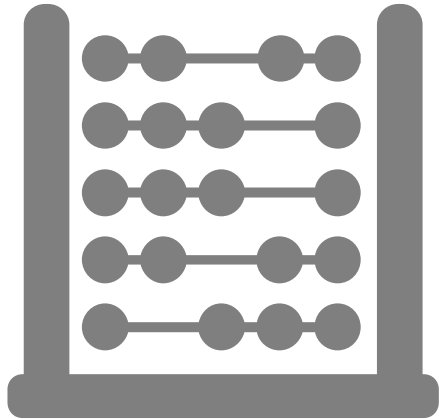




# Similarity: Shifting Focus Towards Value



# Difference: Defining Value



- Senior government leaders want to hear about **Return on investment (ROI)**
- Civilian agencies more likely to have measurements on providing services to citizens
- What about defense...?
- Abstracted away from operations injects **issues determining value**
- Generally, value-based roadmaps don't exist

# Similarity: Cyber vigilance

“Adding Sec to DevSecOps”



# Difference: Pedigree, ATO, and more



- No room for error
- The **lives of citizens and sovereignty** of the nation are at stake
- Authority to Operate (ATO) can take up to 18 months
- Increasing software footprint means increased cyber attack surface
- Understanding software lineage is paramount
- Open Source cannot be adopted without understanding the impact and **intent of contributions**

**Similarity:  
DevOps Requires Trust**



# Similarity: Pride and Passion





Tracy L. Bannon

[TBannon@MITRE.org](mailto:TBannon@MITRE.org)

[TracyBannon@gmail.com](mailto:TracyBannon@gmail.com)

 <https://www.linkedin.com/in/tracylbannon>

 @TracyBannon

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:

<sup>a</sup> 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](http://www.fedweek.com/fedweek/new-data-reinforce-concerns-about-aging-of-federal-workforce).

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

<sup>c</sup>“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](http://changeleadersnetwork.com/free-resources/what-is-transformation-and-why-is-it-so-hard-to-manage). Accessed 29 Nov. 2021.