

# Looking to the Future of DevSecOps and Agile Practices

Atlassian's Insights from the Carahsoft DevSecOps Conference



## Featuring:



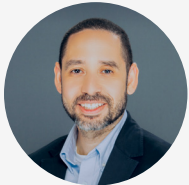
**Ben Straub**  
*Head of Public Sector Sales,*  
Atlassian



**Alex McFarland**  
*Technical Lead,*  
DISA



**Navin Vembar**  
*Principal Engineer,*  
Atlassian



**Arjuna Rivera**  
*Senior Solution Engineer,*  
Atlassian

## Introduction

Agencies are split into various departments and teams. This creates logical groupings of specializations but also instigates the often-discussed problem of organizational silos. As agencies scale and modern technology enables hybrid work environments, these silos have spread to the level of individual workers.

Three departments are central to software development: Development, Security, and Operations. The workflow methodology that fosters seamless collaboration and incident response between these departments is called DevSecOps. This agile way of working splits large chunks of process into bite-sized pieces. From there teams can precisely identify pain points and tackle issues on a small scale, placing solutions ahead of alternatives. The DevSecOps workflow relies on optimizing and adopting agile software solutions. Traditionally, government agencies have hesitated to experiment with commercial platforms, opting for expensive and time-consuming in-house development. This trend has changed over the past 5 years. Commercial platforms now possess security capabilities required by sensitive government work, and more agencies see value in the resources they save.

## What are Misconceptions About DevSecOps?

DevSecOps' agility is misconstrued as chaos. Addressing pain points in real-time results in frequent deliveries and shifts. Adding cross-team participation at every step further blurs lines. While any poorly managed initiative is disruptive, work management tools like Atlassian's Jira Software ensure the detailed tracking and collaborative features needed to make DevSecOps work.

There is also a belief that DevSecOps forces agencies to replace legacy software. While new DevSecOps-compliant tools should be adopted in some instances, the process begins with evaluating and enhancing current operations. Further software adoption comes as needed and is not a must if on-hand tools meet requirements when optimized.

## Why is DevSecOps Such an Important Topic to Government?

Agencies have two workflow objectives: deliver value faster and drive quality up. Stringent regulations and processes force government workers to focus on a narrow set of actions, making them ineffective at delivering what end users need. DevSecOps is innately collaborative. It updates processes and optimizes communication between silos so departments can get back to working toward their primary objective.

DevSecOps is also geared toward continuous evolution. This applies to technology and the people and processes workflows depend on. The needs of governments are in constant flux, as are the skills essential to meet them. Processes by extension must be reevaluated to ensure cohesion within their ever-changing environment. DevSecOps fosters that evolution in a non-obstructive way.



A final point is DevSecOps' approach to risk management. Legacy methods viewed workflows in large blocks separated between departments. This made it difficult to identify why requirements were not met because workers did not have visibility on where mistakes were made. Tuning departments into every part of the workflow, breaking it into small chunks, lets agencies narrow in on exact instances where issues emerge. That precision empowers teams to quickly fix individual broken cogs, rather than invest in a whole new machine.

### How Can Agencies Speed Adoption?

Adopting a new workflow methodology is daunting, but there are keys to ensuring a fast and seamless transition. Leadership plays a critical role in fostering buy-in across departments. Without confidence in change, workers will hesitate to give their best effort. To encourage buy-in, put quality first and speed second. Once the new process demonstrates better outcomes, people will see the efficacy of what you are trying to do. A robust change management framework is also essential, as this shows the importance of DevSecOps on organizational and individual levels.

Having a capable digital services organization within your agency provides a strong advantage when pursuing any modernization effort. The digital service organization has the expertise to fully evaluate software tools. Technical understanding of this nature digs into why something might not work, and what can be adjusted to fix it, rather than tossing things out and moving to the next tool prematurely.

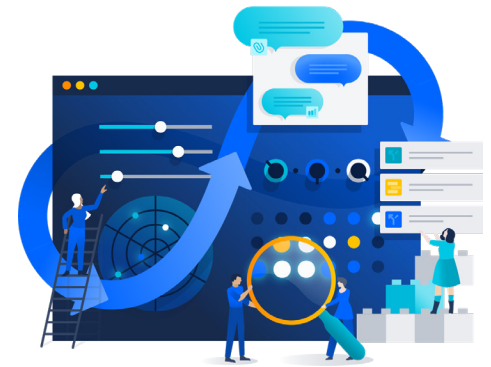
### What are Examples of DevSecOps Working?

There are several places agencies should look to determine whether their DevSecOps initiatives are successful. Improved knowledge sharing is a great start. DevSecOps agencies should notice a greater emphasis on paired programming. Different teams working on separate components of one project should have a deeper understanding of what their colleagues are doing and be able to approach their work with cohesion in mind.

Other areas of improvement agencies ought to track include the following:

1. Are vulnerabilities decreasing?
2. Is uptime improving?
3. Are lead times decreasing?

The primary measure of success is whether end-user satisfaction is improving. DevSecOps' ability to turn feedback into actionable items demonstrates effectiveness to users, strengthening trust and enthusiasm. If this is not the case, your agency must reevaluate.




### Advice From Experts



The mission of government is special, the technology does not need to be. There are methods of delivery and digital tools available on the market that have the capabilities your agency needs or that can lead you to that eventual solution.



Trust the process. DevSecOps has improved leaps and bounds over the last decade and will continue to do so as technology advances.



Do not get intimidated by the goal of perfect architecture. Modernization does not happen all at once. Improve one thing at a time. Automate repeated actions and invest in solving time thieves. Agility is based on the ability to take incremental steps toward substantial outcomes.

### Conclusion

DevSecOps is not contained to the three departments it gets its name from. Every part of the agency is involved. Breaking down silos to this extent seems drastic, but the potential value is significant. Legacy workflow methods suffered from letting poor work accumulate sunk costs until the people who understood the problem eventually got their hands on it. With DevSecOps, that poor work can be spotted and corrected close to the onset.