FEDInsider

Embracing a DevSecOps Culture in Government

People and tools go hand-in-hand when integrating secure software development strategies.

As government agencies adopt DevSecOps to streamline the creation of software and integrate security from the start, they must transform workplace culture to help support the program. At the core of DevSecOps is a team of programmers, system operators and cybersecurity professionals, so it's critical organizations identify the right skills and retrain the existing workforce for program success.

Five security and technology experts in the public and private sector gathered at a recent FedInsider **webinar** to discuss their experiences in building the necessary teams for effective DevSecOps execution.

The following are some of the most important aspects of those efforts.

DevSecOps Is Worth It

DevSecOps adds security into the development process of new software and applications so that by the time software makes it to the production environment, it's already secure. In government, DevSecOps is making meeting security controls easier, so having the right team in place to support it is key.

The U.S Citizenship and Immigration Services began its DevSecOps and agile journey five years ago, and was initially challenged with software version control redundancy. Culturally, it made the shift to software development and DevSecOps to solidify a single platform for version control.

"That platform provided us the capability to do openness, transparency, even collaboration," said Robert Brown, USCIS chief technology officer. Moving forward, Brown said USCIS is shifting from having a DevSecOps team for every contract, to deploying platforms and services at scale to be reused across the organization. The agency is looking towards a culture of openness and collaboration, and tackling security from the framework rather than the tools.

Though modernizing legacy architecture in government can be costly, Taryn Gillison, PEO digital platform application services portfolio manager for the Department of the Navy, said that it doesn't mean agency leads shouldn't start diving into their agile and DevSecOps journeys. In fact, it can help.

"It is not about the tools to develop the framework," Gillison said. "Driving towards automation can allow teams to free up some cycles that they were spending on testing so that they can then focus on modernizing." Then, they can begin to make strides in that area by focusing on the people, processes and cultural shifts needed to modernize.

Cultural Barriers to Achieving DevSecOps Integration

When the Navy embarked on its DevSecOps journey, a task force spent hours interviewing individuals in various stages of the process so leaders could understand where teams thought they were, debunk any myths and help where needed.

"How do we help them go faster? How do we help the other team get to the same common denominator?" Gillison asked.

"We also used it as an opportunity to teach some of the teams who were interviewed about agile because there was still some resistance."

The task force focused on behaviors and practices, culture, technical areas, cybersecurity and policy. This went towards bolstering technical proficiency,

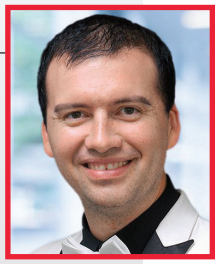
Featuring:

- **Taryn Gillison**
  PEO Digital Platform Application Services Portfolio Manager, Dept. of the Navy

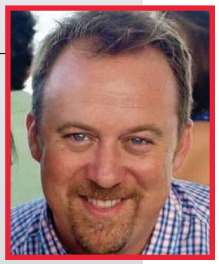
- **Kevin Burnett**
  Technical Director, PEO Manpower, Logistics & Business Solutions, Naval Information Warfare Systems Cmd.

- **Michael Ducy**
  Transformation Specialist, Red Hat

- **Ken Urban**
  Public Sector Solutions Engineer, Atlassian



- **Robert Brown**
  Chief Technology Officer, USCIS



workforce incentives, hiring and retention, and having a unified commander's intent to articulate the near and long term vision for software modernization.

According to Kevin Burnett, technical director and PEO of manpower, logistics, and business solutions for the Naval Information Warfare Systems Command, compliance-focused thinking within cybersecurity can create a cultural challenge, but showing small wins can help.

"The underlying premise is that you have the developing team actively collaborate with security and operations, but in practice, you have a lot of gates," Burnett said. Compliance checking isn't yet an active part of the development cycle, but it needs to be. Burnett recommends picking something small and manageable that is user-engaged to show a desired outcome.

This way, culture can change in smaller groups, and organizations can invest in pilots that demonstrate the efficacy of doing business in this new way. "Then once you have the metrics to prove it, go back and show the larger workforce," Burnett said.

The Proof Is in the Outcome

The old mentality of "if it's not broken, don't fix it" doesn't apply to adopting agile development methods. When Ken Urban, public sector solutions engineer at Atlassian, was working in the intelligence community, his team could no longer wait six months to a year to fix a security patch, so they had to turn to DevSecOps.

"It's all about the mission outcomes. It is not about the software you're building. It is about whether or not you are getting the mission done," Urban said. Focusing on the mission showed senior leaders what worked and what didn't, and gave the team the ability to begin to implement the change that was needed to be able to get patching tasks done in days instead of months.

"You have to do it right, it has to be good showcasing. What you want to do is bring in healthy competition and a desire to emulate from other people," Urban said.

Industry is also leading by example, and demonstrating how a cultural change towards DevSecOps can be beneficial within government. Red Hat, for instance, created the Open Innovation Labs to build real-word experiences and communities of practices within agencies.

"Through the Open Innovation Labs, individuals get the actual experience of working in the DevSecOps model while doing things like continuous delivery and also either working with containers or working with infrastructures," said Michael Ducy, transformation specialist for Red Hat. "This way, they're able to see the efficacy of DevSecOps firsthand."

Getting the Workforce Onboard with DevSecOps

USCIS has seen success in DevSecOps adoption, and to get the organization onboard, Brown said he focused on training, developing teams and promoting the necessary mindset and culture.

"Some of the foundational aspects are full transparency through tooling, deployment, releases, and security with vulnerability and supply chain management — and sharing that information so that it's readily accessible," Brown said.

Burnett also relies on modern hiring practices for workplaces. "We are pushing the envelope wherever we possibly can as it relates to hiring new personnel, but also upscaling existing personnel," he said.

Burnett is leveraging hiring practices from industry to increase interest, and changing the interview process and topics to better meet organizational needs. "Some of the best developers I've met in my career don't even have college degrees," Burnett said. "That needs to be factored into the hiring process as well."

Ultimately, to initiate an internal push towards a DevSecOps culture, experts agree organizations should adopt the cloud, work with industry, embrace autonomy to empower the workforce, take on risk and cultivate an environment of transparency. That is the key to moving government agencies forward into a more agile, DevSecOps environment.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

- (202) 237-0300
- Info@FedInsider.com
- FedInsider.com
- Facebook.com/FedInsiderNews
- Linkedin.com/company/FedInsider
- @FedInsider

carahsoft.

Carahsoft
14993 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Seamus Bergen**

- (703) 230-7425
- DevSecOps@carahsoft.com
- Carahsoft.com/solve/devsecops
- Facebook.com/Carahsoft
- Linkedin.com/company/Carahsoft
- @Carahsoft