Agencies Strive to Create DevOps Culture

The cultural and mindset change required for DevOps is greater than the technological change.

As more agencies begin to adopt the DevOps approach to software development and delivery, they are realizing that building cross-functional teams is the secret to success. This isn't always easy to do though. That difficulty is partly because it requires a significant and department-wide shift in how agencies typically approach software development.

DevOps involves a fully automated, integrated, and continuous deployment process. It helps organizations quickly develop and release software. Agencies can make software changes more frequently to better meet mission requirements and user demands.

For DevOps to succeed, however, agencies have to change the way they think, act, and interact with each other, according to experts speaking at a June 21st event, entitled "DevOps Workshop: Accelerating Development for Mission Success." Changing the culture, they agree, has proven more difficult than the actual technology.

DevOps Still the Goal

If these concerns have agencies wondering whether or not they should adopt DevOps, the answer is still yes, says Mark Schwartz, Chief Information Officer, U.S. Citizenship and Immigration Services (USCIS). "The question is not really whether we are going to implement DevOps; it's are we going to continue to incorporate the practices that are considered good practices," he says. "I think we have a responsibility to the public to do that."

To get the full benefit of DevOps, agencies need to work on fewer projects simultaneously. This can be challenging because government programs are typically massive and consist of numerous requirements. The lack of DevOps expertise—within agencies and the contracting community—can also be an obstacle, he says.

Effective DevOps will require agencies to build a new culture, says Michael Fairless, Branch Chief, U.S. Securities and Exchange Commission (SEC). This culture should empower the skeptics, engage the innovators, embrace the customers, and most importantly, focus on collaboration and teamwork. "If I don't have effective teams, where everyone is participating, where we're engaging even those who don't agree with what we're saying, we can't be successful," he says.

At the USCIS, teams are accountable for the entire process from software development to production. This is a key to success, says Schwartz. "The idea of DevOps is not that you have these different silos working together, it's that you have a cross-functional team."

Typically, the technology side of DevOps has proven much easier to implement than changing the culture, says Leonel Garciga, J6 and Chief Technology Officer, Joint Improvised Threat Defeat Organization (JIDO), Defense Threat Reduction Agency. JIDO looks at gaps affecting the warfighter and typically addresses them at least within two years, so the DevOps approach made sense for the agency.

However, managing risk in this new environment has been a challenge. Agencies must be comfortable with fully automated deployment from development to production without human review, says Garciga.

Risk hampers the ability of an agency to culturally change folks, get IT leadership buy-in, and articulate the security of a system. "How do you automate risk and risk determination? That is an interesting question that is probably where we struggled the most," says Garciga.

For DevOps to succeed, the whole organization must be involved. The Department of Homeland Security (DHS) initially focused too much on the technology. It has since realized that people and processes are just as important, says Rob Palmer, Deputy Chief Technology Officer, Department of Homeland Security. "In order to change culture, you have to engage the people that you're trying to change."

Cloud technology has helped enable DevOps within the DHS. To fully support the DevOps transformation, agencies must build a good foundation to enable new technologies and new approaches, and build a culture around delivery.

Session Highlights
Here are some take-aways from the individual sessions

GOVERNMENT KEYNOTE

The Future of DevOps in Federal IT

Speaker
Mark Schwartz, Chief Information Officer, U.S. Citizenship and Immigration Services (USICS)

Mark Schwartz

"The question is not really whether we are **going to implement DevOps**, it's are we going to continue to incorporate the practices that are considered **good practices**. I think we have a responsibility to the public to do that."

- DevOps involves a fully automated, continuous deployment process that involves cross-functional teams responsible for software development, testing, deployment, operation, and production.

- DevOps is a best practice that should be used widely in government, among other cutting edge practices such as containers, standard set of architectures, and micro-services.

- USCIS offers the full stack of continuous delivery and cross-functional teams and these teams are accountable from development to production.

- The biggest obstacle to DevOps is the lack of experts in the contracting community who can teach agencies how to use this approach. Culture is also a barrier.

- To get the full benefit out of DevOps, agencies need to work on fewer projects simultaneously. Single piece flow is the true DevOps advantage.

CASE STUDY I

Managing Risk in a DevOps Environment

Speaker
Leonel Garciga, J6 and Chief Technology Officer, Joint Improvised Threat Defeat Organization (JIDO), Defense Threat Reduction Agency

Leonel Garciga

"The technology side is super easy. How do you **automate risk and risk determination**? That is an interesting question that is probably where we struggled the most."

- JIDO looks at gaps that affect warfighters and quickly address them at least within two years, so DevOps is a good approach for the agency.

- The agency found its time to deploy was held back by moving to enterprise IT.

- Risk hampers the ability to change culture, get IT leadership buy-in, and demonstrate security.

- It's fine to put software out that's only 20 percent done. Do iterations in real time.

- In the JIDO tenants of secure DevOps, everything revolves around mission.

- Over the last couple years, JIDO experienced a 30 percent cost reduction on the development side.

- DevOps is fully automated deployments from development to production without human review. This forces best practices and prevents human error. Security and compliance are built-in up front.

- In the federal space, the biggest obstacle (other than culture) is lack of DevOps expertise.

TECHNOLOGY INSIGHTS I

Innovating Delivery to Improve Federal Services

Speaker
Craig Schneider, Federal Practice Lead, Excella Consulting

Craig Schneider

"When we're doing **deployments of applications** (and) new features, we are replacing what is out there … with this approach we've been able to introduce new things that **benefit multiple groups of stakeholders** within the agency."

- In one federal agency, the process to deliver new features and enhancements was so long and painful, it was reduced to quarterly releases.

- The 2011 book Continuous Delivery, by Jez Humble and David Farley, gave insights into how to improve and speed up software development.

- It starts with recommending continuous integration, which is a stepping stone to get to DevOps and continuous delivery.

- Excella developers use code branches. Everyone had to merge their code into a common branch multiple times a day.

- The integration is not continuous unless people are integrating throughout the day.

- DevOps has helped reduce the size of releases, increase the frequency of releases, and increase the amount of automation for continuous deployment of features to production four to five times a day.

For more information on FCW Events go to: www.1105publicsector.com/events

Session Highlights, *continued*

The Case for DevOps Culture

Speaker
Michael Fairless, Branch Chief, US Securities and Exchange Commission

Michael Fairless

"If I don't have effective teams—where everyone is **participating** and where we're **engaging** even those who don't agree with what we're saying—we can't be successful."

- The federal government has massive systems and struggles to provide timely services to citizens.

- It took three to five years to deploy DevOps at SEC.

- With DevOps, see the system, focus on the flow, recognize the feedback loops and look for continuous improvement opportunities.

- Challenges to DevOps adoption include maintaining a traditional step-by-step waterfall approach and speaking different languages and terms.

- Effective DevOps requires collaboration, relationships, tools, scaling, and value.

- We can't live in a culture that relies on "that's the way it has always been done."

DevOps Continuous Monitoring; Fail it, Find it, Fix it Faster

Speaker
Brett Hofer, Global DevOps Practice Lead Expert Services, Dynatrace

Brett Hofer

"The name of the game with DevOps for us is to **optimize the lifecycle** of a change."

- DevOps is a cultural and technological shift in how to design, develop, test, provision, configure, deploy, and monitor the entire application lifecycle.

- Agencies are trying to create an agile team where everything is application-centric.

Reward innovation, accept that failures will happen, use mitigation strategies, and have feedback throughout the pipeline.

- Work smarter, not harder, and automate. Innovate more not only with the application itself, but how it is designed, tested, monitored, and delivered.

- Application complexity grows with DevOps, so agencies must have a continuous monitoring system in place.

- Set up an operations center that looks at the entire pipeline, not just the production aspect. Use smart monitoring.

- Dynatrace can track every transaction regardless of the environment and detect problems/failures using smart monitoring for a detailed view of what is happening.

Cloud Foundations for DevOps

Speaker
Rob Palmer, Deputy Chief Technology Officer, Department of Homeland Security (DHS)

Rob Palmer

"In order to change culture, you have to **engage the people** that you're **trying to change.**"

- No matter your role in the organization, it takes all to succeed.

- DHS focused too much on the technology, but now realizes the people and processes are just as important.

- In order to enable transformation, agencies have to build a good foundation that enables new technology, a new approach, and builds a culture around delivery.

- DHS cloud service capabilities start with the foundation of identity.

- Key considerations/challenges include data protection, network, operations and service management, identity and access management, services orientation, data architecture and integration.

- Recommendations include stakeholder engagement, meeting users where they are and working together for a solution, automation, and continuous configuration/authorization that builds security and compliance into development and delivery cycle.

Session Highlights, *continued*

THE WORKSHOP

Speaker
Mark Schwartz, Chief Information Officer, US Citizenship and Immigration Services

Mark Schwartz

"The idea of DevOps is ... that you have **a cross-functional team.**"

· The relationship between the federal government and contractors is one that requires feds to give constant meaningful feedback.

· Peer code reviews should happen before code is checked in and approved, which is when automation takes over.

Speaker
Leonel Garciga, J6 and Chief Technology Officer, Joint Improvised Threat Defeat Organization, Defense Threat Reduction Agency

Leonel Garciga

"**Shift your mindset** on what testing and user testing looks like because the user is **actively part of that team** already."

· With DevOps, don't bite the whole apple. Do it in small chunks.

· Government isn't set up to support the more common sense approach to addressing requirements that DevOps allows.

· How to do DevOps at scale at an enterprise level is the challenge.

Speaker
Craig Schneider, Federal Practice Lead, Excella Consulting

Craig Schneider

"There has been a great shift in focus to ... getting t**hird party opinion** and **peer reviewing code.**"

· Within the DevOps model, enterprise architects are working with the teams, not in another organization.

· Having a second set of eyes on coding issues from outside of the development team is helpful.

Speaker
Michael Fairless, Branch Chief, US Securities and Exchange Commission

Michael Fairless

"The challenges I had with security two years ago ... [were] **much more significant than they are today**."

· The challenge with security is getting everyone on board; you have to put security into this mentality.

· Deploy software to a small group first, and then ramp up to full deployment.

Speaker
Brett Hofer, Global DevOps Practice Lead Expert Services, Dynatrace

Brett Hofer

"In DevOps, there are a series of techniques called **canary releases** [targeting] a limited set group ... **to control** [the impact of code changes.]"

· In DevOps, there are techniques called canary releases sent to a limited user group, and dark launches where features are introduced under the hood without anyone seeing them.

· DevOps also helps agencies monitor and flag something as they monitor the environment.

Speaker
Rob Palmer, Deputy Chief Technology Officer, Department of Homeland Security (DHS)

Rob Palmer

"From the top down, we should be **driving towards DevOps focused architectures** or at least DevOps enabling architectures."

· DevOps and enterprise architecture are closely tied, but the models are struggling with how to get to DevOps focused on enabling architectures.

· From the top down, agencies should be focused on DevOps enabling architecture.

BUILDING DEVOPS CULTURE

3 Keys to Building a Federal DevOps Culture

DevOps is certainly not new, but it is becoming more important every day. This is especially true in federal IT. The private sector has embraced DevOps, and it has changed the way businesses operate.

It's been six years since the first DevOps Day in Europe, and its influence has spread around the world. In that time, the end of isolation between development and operations teams has paved the way for commercial organizations to turn out better software more quickly and to achieve new levels of quality and efficiency.

Unfortunately, those successes have not translated to federal agencies. The 18F program, with its support of agile software delivery, is an enormous step in the right direction, but there are still critical barriers to overcome if agencies are going to adopt true DevOps cultures.

DotShock/Shutterstock.com

DEVOPS PRACTICES

DevOps—the Next "Best Practice" for Government IT

DevOps is a culture, as much as it is a philosophy, as much as it is a method of continuous improvement in software applications. It may be the first manifestation in the government IT world of the impact of millennials' views of the world—fast, repetitive, automated, collaborative, less risky, small-scale—but with a collective big impact and a permanent change to how organizations think about infrastructure investment.

That may explain why the government speakers at the Advanced Technology Academic Research Center's (ATARC) first DevOps Summit in Washington, D.C. were less formal and more irreverent about the mainstays of government contracting, such as defining requirements and Firm Fixed Price.

First, an explanation: DevOps, from Development and Operations, is based on the idea that bringing together employees who develop solutions with employees who perform the mission will encourage collaboration on ideas that actually improve how people do their day-to-day jobs. A big part of making DevOps work is automating as much testing as possible, whether it's for functionality, security, Section 508 compliance, load balancing, and so on. Automated testing is a crucial part of DevOps because software updates for improved or new functionality are released often – in many cases, once a day – so testing the software has to happen just as quickly.

"I like to think of DevOps as today's best practice," said Mark Schwartz, CIO for U.S. Customs and Immigration Services. "We're using DevOps everywhere we can … We have a number of new systems that we were able to 'greenfield' with the DevOps approach. [Then] we have legacy systems where we're using the strangler approach."

Sharomka / Shutterstock.com

FEDERAL DEVOPS

Bringing DevOps to the Federal Government

Forgive federal CIOs if they feel a little trapped. Agencies face enormous budget challenges and increased citizen service expectations, yet they have to execute their IT game plans within software development models built for the 1980s. Traditional approaches were created with the best of intentions—incorporating the insight of a number of disparate internal stakeholders (developers, testing groups, change management committees) to provide checks and balances during system development.

It looks great on paper, but in reality, these stakeholders end up batting risk back and forth like a volley ball; and the collective group becomes less concerned with outcomes. The result? Time is lost, taxpayer dollars are wasted, and systems that commercial organizations can roll out in months take years for agencies to deliver. In the current "Cloud First" federal IT landscape, a DevOps operating model has become a necessity.

DEVOPS SECURITY

With DevOps Security Must Work Differently

Because "software is eating the world," as Mark Andreessen famously noted, application security gets harder every day. Every line of code written opens organizations to new vulnerabilities and breaches.

Furthermore, legacy solutions, such as static analysis, dynamic analysis and web application firewalls have failed to keep pace with Agile and DevOps practices. Teams need tools that empower developers, integrate security into the DevOps toolchain, and monitor application security the way DevOps teams monitor application performance.

DEVOPS AND COMPLIANCE

Why Compliance Demands a DevOps Approach

Stop me if you've seen this scenario before: A compliance policy is developed behind closed doors by federal security advisors. Once published, it's sent to IT managers, who take one look and think, "Well, this won't really work."

They begin the arduous process of trying to provide feedback, which amounts to submitting a request into a suggestion box, and waiting for an answer that may or may not come. The public comment process is often opaque; you don't know if or why your comments were rejected and it's difficult to appeal your case.

This classic "waterfall" approach to the creation of security and compliance procedures is in direct contrast to the fast and agile DevOps approach to application development that many agencies embrace today. Over the past few years, the federal government has turned to Silicon Valley startups filled with former Presidential Innovation Fellows to bring agencies into the 21st century. These people understand the value of DevOps development principles, but they've been asked to meld those principles with an antiquated waterfall security process with gated checkpoints, starts-and-stops, and long development cycles.

DEVOPS CULTURE

DevOps Becomes Increasingly Common Inside Government

Silicon Valley-style culture at the stodgy Department of Homeland Security? It's no joke, said Barry Crist, CEO of server automation software company Chef, after recently visiting DHS' IT shop. "It felt and smelled like a Silicon Valley startup," Crist told FedScoop at Amazon Web Services' recent re:Invent conference.

Since DHS' IT shop adopted agile and DevOps development methods, it radiates a startup atmosphere, Crist said. And DHS is not alone. Over the past two years, he's seen agencies across government take to private sector techniques with gusto.

"There used to be this chasm between what was going on in industry and what was going on in the public sector," he said. "The agencies that are doing the most forward-looking things are matching what's going on in the most forward-thinking enterprises." Crist's sentiments come after seeing how the U.S. Citizenship and Immigration Services improved how it processes immigration records. His company also has helped Department of Energy's National Renewable Energy Laboratory embrace DevOps by automating its security controls when it configures its servers.
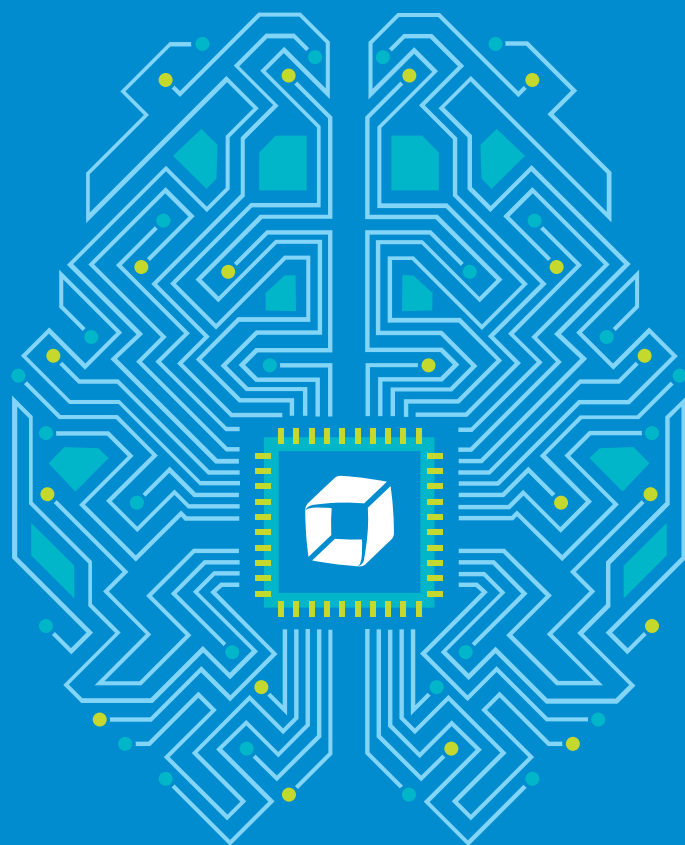
Chris Webber, the chief cloud architect at NREL, said the speed that comes with these services, along with the agile development culture, is something the government throughout needs to adopt.

For more information on FCW Events go to: www.1105publicsector.com/events