Q&A

Executive Viewpoint

A conversation with Robert Vietmeyer

Director for Cloud and Software Modernization, Office of the Deputy CIO for Information Enterprise, Defense Department

This interview continues at Carah.io/2022-FCW-Aug-Cloud.

How is DOD speeding the deployment of cloud technology while still adhering to the department's strict security requirements?

We have a two-part approach that aligns with the shared responsibility for cybersecurity in the cloud. The cloud service providers are responsible for securing the cloud infrastructure, and the customers are responsible for securing their applications and data within the cloud. We started with programs like FedRAMP and our DOD provisional authorization process, which was focused on establishing secure baselines for commercial cloud services, accrediting those services across those baselines and allowing anyone in the department to access the services without the need to do their own assessments. We have been working with the commercial cloud service providers for many years and have seen the improvements in their cybersecurity infrastructure, and the services they're providing continue to mature and improve over time.

Now the biggest risks in the cloud aren't coming from the cloud infrastructure. They're coming from misconfigurations in how users are securing their applications and workloads in the cloud and meeting their responsibilities for cybersecurity. So we have shifted our focus to provide additional guidance to DOD cloud users on how they should secure their applications and data when they're operating in the cloud. For instance, we've recently published infrastructure-as-code scripts that we cooperatively developed with the major cloud service providers under cooperative research and development agreements. We've created secure configurations that can be deployed in a matter of minutes or hours and that would normally take a program that's just getting started about seven months or more to establish.

We can now give them software that will go into the cloud, establish the right cloud services, configure them appropriately and then apply cybersecurity policies consistently across that entire configuration. Within minutes, users can push a button using these infrastructure-as-code scripts and get a secure cloud configuration that meets DOD cybersecurity requirements and allows them to continually monitor their cyber posture over time. It's a powerful, powerful capability.

We're also working on the extension into DevSecOps and platform engineering, and we're providing additional guidance on building resilient cyber platforms in cloud environments through our DevSecOps efforts.

Why has DOD shifted its cloud strategy to a Software Modernization Strategy?

We are now in our third iteration of cloud strategies at the department, and each one

> **The biggest risks in the cloud aren't coming from the cloud infrastructure.** They're coming from misconfigurations in how users are securing their applications and workloads in the cloud."

> The realization that **cloud computing is a journey and not a destination** is fundamental, and so is the need to anticipate and plan for ongoing change."

has mapped to the phases of maturation we've gone through. The first cloud strategy focused on efficiency and data center optimization while we were learning about cloud and shifting from capital expenditures to operating expenses.

The second phase was about contracting optimization. We found that as folks moved into the cloud, there was a proliferation of contracts, making it a suboptimal approach. So we asked: How do we start to integrate our approach to contracting and delivery? How do we start to build out organizations that can help customers be more successful in moving into the cloud? That consolidation has led to a handful of core cloud contracts that are operated by the military departments, with the Defense Information Systems Agency being the key focus area for contracting and moving DOD customers into the cloud.

The third phase, which we're in now, is about integrating the cloud into our software modernization approaches around DevSecOps. The focus now is on the mission. How do we leverage cloud as a core component of our IT infrastructure and use that as a foundation for delivering continued innovation, advanced mission capabilities and improved cyber resilience? We have moved beyond just getting into the cloud to consider how to use the cloud effectively and re-engineer our applications and processes to make sure we're delivering what end users and the mission need.

How is DOD revising acquisition and budgeting processes to achieve its cloud and software modernization goals?

We have a great partnership with our counterparts in the Office of the Undersecretary of Defense for Acquisition and Sustainment, which issued the software acquisition pathway process, DOD Instruction 5000.87. This is a new, foundational acquisition process for how the department is moving forward and innovating its approach to IT delivery. With the pathways, we're able to remove the traditional acquisition milestones that had been designed around a waterfall approach and replace them with a two-phase acquisition process — a rapid planning phase followed by an ongoing iterative delivery phase. This new process facilitates the rapid, iterative development and the ongoing delivery of capabilities to the end user by integrating modern software development practices such as agile, DevSecOps and lean practices directly into our acquisitions.

Now we're working with DOD components and our program managers to improve our understanding of how we can make the transition from the way we have been doing business to this modern way that's enabled by the software acquisition pathways and supported by the technical components and guidance from the DOD CIO.

What advice do you have for other agencies on how to make the best use of cloud technology?

The realization that cloud computing is a journey and not a destination is fundamental, and so is the need to anticipate and plan for ongoing change — not just at the technology level, but also in terms of your internal policies, your processes and your workforce. We have found that taking maximum advantage of the cloud to drive continued innovation, improve cybersecurity and expand our agency's capabilities requires a comprehensive look at and change across the entire culture of IT delivery and use.

My advice would be that if you haven't started, get started. Begin with low-risk systems, build from there, and try to leverage to the maximum extent possible the experience and guidance of those who have done it multiple times before. The cloud is a complex environment. Each of the major providers has hundreds of different services that need to be correctly configured, deployed, operated and maintained to avoid exposing yourself to unnecessary risk.

What we're seeing at DOD is that the next important step is the adoption of DevSecOps and platform engineering, which allows us to start to scale the delivery and value proposition of cloud so that each program doesn't have to figure this out for itself. Instead, we can engineer advanced, cloud-based, resilient platforms and deliver them as a service to multiple application development teams. We can separate the teams that specialize in the delivery, security, ongoing efficiency and performance improvements at the platform level from the application development teams, which frees those developers to focus on delivering ongoing innovation and best value to the user community.

Based on our experience at DOD, the key is to shift from thinking of cloud as a technology to thinking of cloud as an enabler for the next steps. ■