



Setting Up DoD-Compliant Cloud Made Simpler with AWS GovCloud

As the Department of Defense (DoD) moves from a primarily on-premises IT environment towards a cloud-native one, one question has been top-of-mind at the agency: How can cloud providers create a cloud environment for government use that is compliant with stringent regulations at the Pentagon?

Amazon Web Services (AWS) aims to do the lion's share of the work in that cloud journey, with its AWS GovCloud (US) solution capable of doing 60 percent of the work, company officials said at the AWS Summit Washington, DC in 2021.

"The compliance framework is that landing zone that you can deploy in AWS GovCloud (US)—the secure, compliant, multi-account foundation that exists in GovCloud," Jim Collins, an AWS security leader, said at the summit.

The "landing zone," as Collins called it, is a starting point for new development and experimentation, and also where organizations should start when migrating applications to the cloud. The environment also allows for both iteration and extension over time.

With an enhanced focus on cybersecurity requirements in federal government environments, the AWS GovCloud (US) gets DoD customers most of the way there, at least in terms of the security controls provided.

That landing zone required to be deployable on AWS infrastructure is hosted within the continental United States, and operated by American citizens. The landing zone is essential, and is a secure and scalable multi-account AWS environment.

AWS GovCloud (US) complies with the Federal Risk and Authorization Management Program (FedRAMP) moderate and high requirements, the DoD's cloud security guide, Defense Federal Acquisitions Regulations Supplements, and the National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-171. AWS GovCloud (US) is set up to accelerate implementation of a compliant cloud environment, the AWS officials said.

"There are several things that this environment enables," said Randy Domingo, senior consultant for worldwide professional services at AWS. "First, because we are enabling organizations, you can take advantage of

consolidated billing, and you can take advantage of AWS's ability to deploy guard rails into your accounts via service control policies."

Beyond that, Domingo said the AWS GovCloud (US) environment allows users to share resources with each other, and its architecture puts the central account in charge of all account provisioning, as well as the service catalog.

"It also allows you to be able to share different resources with all the different accounts here," Domingo added.

"Whether that be easy-to-use snapshots or setting up an Amazon Machine Image (AMI) pipeline, or [...] ensuring a networking stack or transit gateway, which provides kind of the network fabric between your mission applications or tenant accounts and the shared services within our management services and our transit account," he continued.

The AWS DoD compliant framework takes the burden of setting up a cloud-native environment off of the government and contractors and leaves account administrators and managers with just the work of managing personnel and incident response.

The framework's long-term benefits include the ability to extend the AWS-compliant environment to include additional services as necessary, depending on mission needs. Any additional services needed are simply layered on top as organizations build out the structure of their cloud environment to fit their mission needs.

"When we look at the shared responsibility model, there is the foundational thing that AWS as a whole goes in and provides, and then there's what you, as a customer, are responsible for doing," Domingo said. "We're trying to make a lot of the decisions that help with the decision-making there by providing the prescriptive guidance for that next layer up—which is a compliant framework—to then allow you to be able to go do what I call are the sharp edge missions."

Whether it's adding on Amazon Workspaces, artificial intelligence or machine learning, a DevOps pipeline, or a data lake, AWS's compliant cloud is able to add services on as mission requirements grow, the company officials said.