



# Cloud security considerations for DOD mission partners



**Jeffrey Phelan**

milCloud® 2.0 Cloud Services Portfolio Lead, GDIT

DOD mission partners benefit from a fit-for-purpose cloud that offers the highest levels of security

**M**OVING TO THE CLOUD REQUIRES a considerable level of effort and expense. Ensuring the security of applications or services running in a cloud adds another layer of complexity. When choosing a cloud service provider, organizations need to understand what security controls they will effectively inherit from that provider and what controls they will have to build and deploy on their own.

For government agencies, FedRAMP provides a host of security levels and a robust number of security controls in a well-documented package, but Defense Department agencies also need to understand if they have any additional impact-level requirements for their applications and mission-critical data. As mission partners move to the cloud, they need to make sure that approved cloud providers can meet those baseline security and impact-level requirements.

Many organizations or application owners may lack the internal capability to bridge security gaps that may occur when moving from an on-premises data center to a commercial cloud. Additionally, the traditional acquisition process can be cumbersome and time-consuming and can significantly delay your move to the cloud. The Defense Information Systems Agency's "fit-for-purpose" cloud service, milCloud® 2.0, eliminates this costly additional process by allowing DOD mission partners to buy cloud consulting, expertise, engineering and technical support with the infrastructure as a one-stop shop.

## Connecting cloud offerings to DOD networks

DOD has taken a comprehensive approach to making sure its agencies can operate securely in the cloud. The ability to meet very rigorous security requirements relies heavily on clear policy directives and well-documented processes and procedures as contained in DOD's Cloud Computing Security Requirements Guide.

General Dynamics Information Technology powers milCloud® 2.0, which connects cloud service offerings to DOD networks. milCloud® 2.0 gives our mission partners the ability to inherit a baseline set of security controls that differs significantly from what other commercial or custom-built clouds can offer.

## A wealth of security controls

Beyond inheriting the security controls of the DOD networks, mission partners also inherit the physical controls from the DISA data centers and the military bases where they reside. Additionally,

they acquire the controls from DISA's internal cloud access point, as well as milCloud® 2.0's Impact Level 5 authorization from DISA and our FedRAMP High authorization.

This robust security inheritance is delivered within that Impact Level 5 cloud service, which scales on demand. This makes it a cost-effective solution for DOD mission partners that is available today using MIPR funds or a credit card, delivering a cost-effective, convenient and secure cloud service to DOD. ■

**Jeffrey Phelan** is the milCloud® 2.0 cloud services portfolio lead at General Dynamics Information Technology.

**milCloud<sup>2.0</sup>**  
© Powered by General Dynamics Information Technology

Because the mission matters.  
Today.

[LEARN MORE](#)