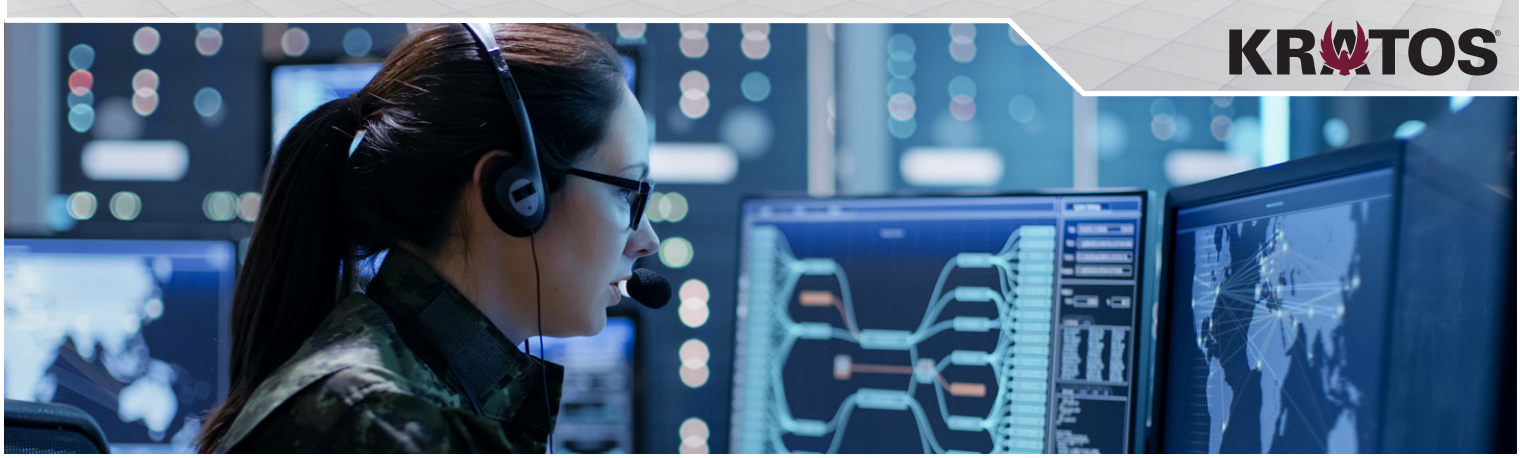
Open the Door to the DoD Market with a Kratos DoD SRG Assessment



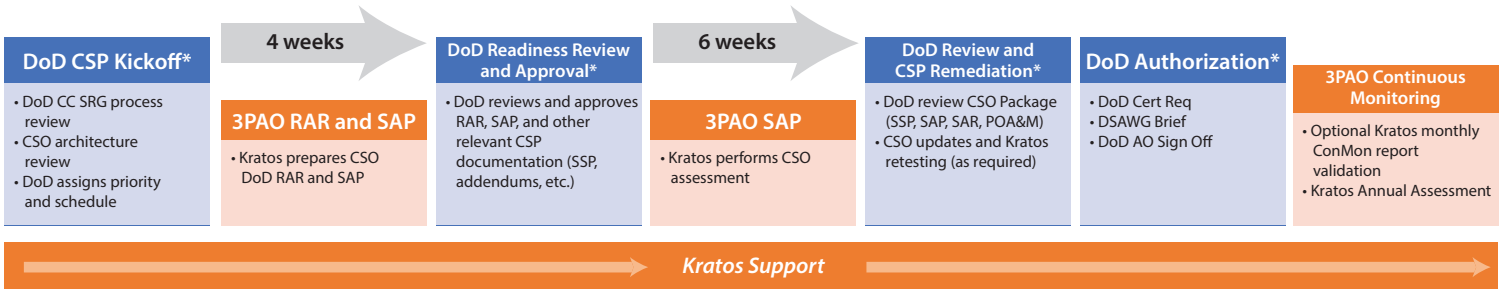
As DoD Applications and Services migrate from Department of Defense (DoD) owned and operated data centers to commercial cloud services, Cloud Service Providers (CSPs) have an opportunity to break into or expand their footprint within the Federal space by demonstrating that the offering meets DoD Cloud Computing (CC) Security Requirements Guide (SRG) requirements.

The DoD CC SRG requirements are built on a FedRAMP foundation and typically leverage an existing FedRAMP authorization. As an authorized FedRAMP Third Party Assessment Organization (3PAO), Kratos follows its proven methodology for FedRAMP assessments to determine whether a CSP's offering meets the more stringent DoD CC SRG requirements.

Save Time and Money

The DoD reciprocity with FedRAMP may not always be clearly defined or understood by CSPs. Leveraging Kratos' experience enables efficiencies to be brought forward and brokered with DoD. These efficiencies include limiting the scope of the assessment to the deltas between the DoD CC SRG security controls and parameters and FedRAMP security requirements. Doing so has the potential to reduce the scope of or even eliminate required artifacts. This approach can save time on delivery (due to fewer number of security controls being tested) and reduce costs for the customer (due to resulting reduction in overall level of effort).

Kratos provides assessment services to CSPs seeking DoD Provisional Authorization (PA) from the Defense Information Systems Agency (DISA) at Information Impact Levels 2 through 6 (IL2 - IL6). Kratos employs cleared individuals to support DoD engagements when required (e.g., IL6).



* Refer to the DoD Authorization Process for additional detail on process, interactions and timelines.

Kratos DoD CC SRG Assessment Process and Timeline

Phone: (719) 598-2801 • EMail: Space@KratosDefense.com • Web: www.KratosSpace.com

Kratos has established strong relationships within the DoD, DISA, FedRAMP Program Management Office (PMO), FedRAMP Joint Authorization Board (JAB), 15+ authorizing agencies, and many of the world's largest CSPs. These relationships are invaluable when interacting with Authorizing Officials (AOs). Kratos has exhibited success at the highest levels by assessing one of the largest and most complex CSPs and achieving one of the first DoD ATOs issued to a commercial cloud provider. Kratos continued this success by performing the first IL6 assessment for a commercial CSP, which was successfully adjudicated at the Secret level. These engagements enabled Kratos to work alongside DoD stakeholders to lay the groundwork and establish many of the processes that remain in place.

Build a Trust Relationship with AOs

CSPs can trust that Kratos' comprehensive assessment methodology and knowledge of the DoD CC SRG requirements and processes will result in an efficient and streamlined cloud authorization process. Kratos services will identify, analyze, and provide recommendations to mitigate risks and vulnerabilities that could potentially put the CSP and hosted customers at risk. The resulting Security Assessment Report (SAR) will provide detailed insight into any identified residual risk within the CSP's processes, technologies, and architecture. Kratos will work with the CSP to gain and present a risk posture to enable quick and informed decisions by AOs.

Benefits of a Kratos DoD CC SRG Assessment

- Strong relationships with the DoD CC SRG and FedRAMP stakeholders can accelerate a CSP's time to market
- First 3PAO to perform an IL6 DoD CC SRG assessment for a commercial Cloud Service Provider
- Maintain cleared staff to support DoD engagements
- Extensive understanding of DoD acceptable control implementation expectations
- Strategic insight into performing uplifts to DoD CC SRG Impact Levels to reduce overall effort and time to authorization

About Kratos Cybersecurity Services

Kratos cybersecurity services support the development and operation of proactive cybersecurity programs, the development of enterprise cloud security strategies, and the establishment of sound and practical information security architectures tailored to organizational needs. With years of robust compliance and certification experience in government and commercial standards requirements as an authorized FedRAMP 3PAO and more recently, a Cybersecurity Maturity Model Certification (CMMC) C3PAO, Kratos is viewed as a trusted compliance and governance partner by the DoD, Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.