



The Department of Defense Introduces Cybersecurity Risk Management Construct (CSRMC) to Enhance Cyber Defense

October 10, 2025

Reading Time : **1 min**

By: Evan D. Wolff, Rita S. Heimes, Maida Oringher Lerner, Marta A. Thompson, David A. Mahoney

The Department of Defense (DoD) has introduced the Cybersecurity Risk Management Construct (CSRMC), a new framework that replaces the legacy Risk Management Framework. CSRMC emphasizes automation, continuous monitoring, and real-time visibility, marking a significant shift away from static, checklist-driven processes.

This change is likely to have implications beyond DoD systems, particularly for contractors who may be required to provide real-time monitoring data or other evidence to support oversight in the future. While CSRMC does not replace the Cybersecurity Maturity Model Certification (CMMC), it signals a broader shift in the DoD's approach to risk management and contractor expectations.

Click [here](#) for more information.

Categories

Compliance

Cybersecurity, Privacy & Data Protection

Consumer Privacy

Related Content

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.