wiley

ALERT

FedRAMP Announces New Approach to Assessing Security of Cloud Services Providers, Leveraging Commercial Practices and Tools

March 27, 2025

WHAT: FedRAMP has announced that it will be working on a new framework for authorization and assessment of cloud services for federal consumption, calling the initiative "FedRAMP 20X" (announcement here). In response to concerns from cloud service providers (CSPs) and other stakeholders that the existing FedRAMP process is too expensive, time-consuming, and challenging, FedRAMP 20X aims to improve the efficiency of the FedRAMP process by "transitioning away from costly, inefficient, manually compiled documentation and towards industry-led, data-driven security reporting." To meet this objective, the new framework will focus on five specific goals: (1) simplify application and validation of security requirements through automation; (2) leverage commercial security frameworks and investments; (3) progress continuous monitoring to a more "hands-off approach"; (4) lean into the direct business relationships between providers and customers to build trust; and (5) enable rapid improvements by reducing "artificial checkpoints."

WHEN: FedRAMP announced that it expects to launch four Community Working Groups (CWGs) to develop FedRAMP 20X in the next month:

- Rev5 Continuous Monitoring (March 31, 2025). This group will work on developing a standard for continuous monitoring reporting by CSPs.
- Automating Assessments (April 2, 2025). This group will focus on developing standards and tools to automate assessment,

Authors

Kevin J. Maynard
Partner
202.719.3143
kmaynard@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity

Government Contracts

reporting, and enforcement of technical controls.

- Applying Existing Frameworks (April 8, 2025). This group will examine industry-leading security standards and evaluate opportunities to leverage commercial frameworks to reduce government-unique or redundant compliance mechanisms.
- Continuous Reporting (April 10, 2025). This group will work on methods to allow ongoing risk monitoring to be enforced, validated, and reported continuously, resulting in reports to customers that reflect near-real time risk posture.

The technical assistance and guidance the CWGs develop with public input will be formalized on a "rolling basis" and will go through "formal public comment" before becoming official.

WHAT IT MEANS FOR INDUSTRY: The FedRAMP 20X initiative is intended to address industry and stakeholder feedback that the FedRAMP authorization process is resource-intensive and time-consuming, while also aligning with the Trump Administration's emphasis on government efficiency and "industry-led, data-driven security reporting." See FedRAMP 20X FAQs.

The announcement of FedRAMP 20X identifies several key changes from the current FedRAMP authorization and assessment frameworks. One of the most notable changes is a reduction in the amount of required documentation and an increased emphasis on using technology and tools to automate assessments, security validation, reporting, and/or the enforcement of technical controls. While the details are yet to be worked out, the announcement promises that new documentation required for FedRAMP will be reduced to a few pages, and that 80% of security requirements will be addressed through "automated validation" without the need to write a single word about how it works – compared to the current FedRAMP process, which requires narrative explanations for 100% of the current security requirements.

Another notable aspect of FedRAMP 20X is the plan to rely on industry and "commercial best practices" to "create innovative solutions" that meet the government's minimum security standards. To that end, the CWGs will hold regular public meetings and provide a shared workspace where industry and other stakeholders can provide input into the development of the new standards. Each piece of guidance will go through formal public comment, and will be updated on an annual basis, providing a further opportunity for industry to help establish standards.

Finally, the new process will eliminate the need for an agency sponsor, which under the current process can be a challenge for new entrants into the federal market. Currently, those seeking authorization must establish partnership with a sponsoring agency, undergo a full security assessment, and – after authorization – must participate in continuous monitoring and annual assessments by FedRAMP. Under FedRAMP 20X, this sponsorship requirement will be eliminated, and CSPs will instead be able to submit documentation and automated validation directly to FedRAMP to be added to the FedRAMP Marketplace (FedRAMP 20X One-Pager).

According to the announcement, these and other promised changes will help reduce the burdens on CSPs and shorten the time required to obtain FedRAMP certification from months to weeks. The announcement does not include a timeline for the CWGs to begin issuing new standards and guidance. In the meantime, for CSPs currently pursuing or interested in pursuing authorization in the near term, FedRAMP intends to maintain the existing Agency Authorization path while working on FedRAMP 20X. After March 31, 2025, however, the FedRAMP Program Management Office will no longer: provide updated technical assistance or implementation guidance for the Rev5 baselines; perform "triple check" reviews of FedRAMP Rev5 packages; or perform centralized continuous monitoring of cloud service offerings that had been authorized by the former Joint Authorization Board (JAB) (FAQs).

Wiley's multidisciplinary Government Contracts and Cybersecurity teams will be monitoring these and further developments.