wiley

ALERT

FedRAMP Issues Final Proposed Changes to Cloud Authorization Process, Seeks Comments from Industry

January 23, 2026

WHAT: The FedRAMP Program Management Office (PMO) has released a "final set" of proposed changes to the FedRAMP process for authorizing and assessing the security of cloud services for federal consumption. The final proposed changes, issued this month after extensive engagement with industry over the past year, cover six separate aspects the FedRAMP process. The FedRAMP PMO is seeking public comment before adopting these changes (see announcement here).

WHEN: The final proposed changes to the FedRAMP process have been released in six separate proposed policy changes and requests for comment (RFCs), with the following staggered deadlines for interested parties to submit comments:

FedRAMP also expects to host a Q&A session on the proposed policy changes and RFCs, with the date and time to be announced.

WHAT IT MEANS FOR INDUSTRY: As we previously reported (see here), the FedRAMP PMO has been engaged in a year-long effort – known as "FedRAMP 20X" – 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." This effort was undertaken in response to direction from Congress and the Office of Management and Budget, as well as feedback from cloud service providers (CSPs) and other stakeholders that the original FedRAMP authorization process was too resource-intensive and time-consuming. Over the past year, the FedRAMP PMO has solicited additional feedback from industry and

Authors

Kevin J. Maynard
Partner
202.719.3143
kmaynard@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Government Contracts

other stakeholders, through "Community Working Groups" organized to address various aspects of the FedRAMP process. These efforts have culminated in the final proposed changes set forth in the six RFCs, which include the following notable changes to the FedRAMP process:

- **RFC 0019: Reporting Assessment Costs**
  As directed by Congress in the FedRAMP Authorization Act, Pub. L. No. 117-263, § 5921 (2022), the FedRAMP PMO is proposing to require CSPs to provide the FedRAMP PMO with information regarding the effort and cost incurred by CSPs to engage third-party assessment organizations (3PAOs) in achieving FedRAMP certification (initial and annual). According to the RFC, this data is needed to comply with the FedRAMP Authorization Act, and to help the Government to understand the impact of ongoing changes to the FedRAMP assessment process.

  The RFC acknowledges that the requested cost information may be considered sensitive by CSPs and 3PAOs. The RFC also indicates that the FedRAMP PMO will not share any cost data, or the name of the CSP or 3PAO, "unless legally required," and will "take steps to avoid de-identification reversal when sharing cost data." Finally, the RFC specifically invites interested parties to comment on the potential impact of collecting, reviewing, and sharing the requested cost information.

- **RFC0020: FedRAMP Authorization Designations**

FedRAMP proposes to clarify program terminology by coining new, distinct terms for different types of FedRAMP "authorizations." FedRAMP anticipates launching the updated terminology in March 2026.

-
  - "FedRAMP Certified" indicates that the service has completed a point-in-time assessment. More specifically, it would designate a service that has completed a point-in-time FedRAMP assessment that meets the legacy FedRAMP Rev5 requirements and is therefore considered "FedRAMP authorized."
  - FedRAMP Validated" indicates that the service has undergone an assessment of its processes to ensure it will persistently meet security requirements. More specifically, it would designate a service that has demonstrated the ability to persistently validate their security posture to FedRAMP. FedRAMP has assessed the process used by the service provider and ensured there is sufficient information in the persistent assessment materials to be used by agencies in making ongoing authorization decisions. A FedRAMP Validated service would likewise be considered "FedRAMP authorized."

- **RFC0021: Expanding the FedRAMP Marketplace**

FedRAMP proposes to allow cloud service providers to list cloud service offerings while preparing to obtain a FedRAMP Certification or Validation, a change from the current model where offerings are only listed in the FedRAMP Marketplace after obtaining authorization. FedRAMP intends for this update to allow industry and agencies alike better insight into where different service offerings are on their respective paths to obtaining

FedRAMP Certification or Validation.

FedRAMP would also allow assessors and advisory services in support of FedRAMP to be listed on the Marketplace.

- **RFC0022: Leveraging External Frameworks**

FedRAMP is proposing to provide a temporary, expeditious path for cloud services to obtain a Level 1 FedRAMP Validation through its FedRAMP 20X validation program. To qualify for a Level 1 Validation, the cloud service must: be listed on the FedRAMP Marketplace; have completed an external security assessment from a list of existing frameworks (including SOC 2 Type II and CMMC Level 2), and make full materials from that assessment available to those necessary to achieving the Validated Level 1 authorization package; provide a temporary mapping from the existing security assessment to a subset of FedRAMP key security indicators; and submit a Validated Level 1 authorization package.

The Level 1 Validation is intended only for agency use. FedRAMP also proposed updates to the Minimum Assessment Scope for both FedRAMP Rev 5 and 20X materials to clarify the Level 1 Validation framework.

- **RFC0023: Rev5 Program Certifications (No Sponsor Required)**

FedRAMP proposes to address some of the authorization backlog by offering a time-limited opportunity in this calendar year for cloud service providers who have demonstrated substantial progress towards a Rev5 Certification to obtain program authorizations for FedRAMP Certification at Levels 1-4. Among other things, providers would need to implement all legacy Rev5 requirements at the appropriate impact level, meet requirements and recommendations from FedRAMP's Rev 5 Machine-Readable Packages, complete a full FedRAMP assessment with a "trusted assessor," and submit a complete authorization package no later than December 16, 2026.

- **RFC0024: FedRAMP Rev5 Machine-Readable Packages**

FedRAMP proposes to modify the Rev5 process for current and future Rev5-based assessments and authorizations to require cloud service providers to ensure data provided to FedRAMP is machine-readable in the hopes of streamlining FedRAMP authorization processes and review. FedRAMP seeks comment on the specific proposed requirements for the machine-readable packages and anticipates making any requirements effective September 30, 2026. After a one-year grace period, any service that does not comply with the data submission requirements may lose FedRAMP Certification.

* * * *

The final set of proposed changes to the FedRAMP process and the accompanying RFCs provide CSPs, 3PAOs, and other interested stakeholders with a final opportunity to provide input on these important changes to the process for authorizing and assessing the security of cloud services for use in the U.S. Government marketplace. With the Government's continued focus on cybersecurity compliance, and the risks of

noncompliance (including risks under the False Claims Act, as discussed here), providers and users of cloud services in the U.S. Government marketplace should make sure they stay up to speed with these changing requirements to ensure they remain in compliance.

Wiley's multidisciplinary Government Contracts and Cybersecurity teams have extensive experience advising clients on various issues relating to FedRAMP and other security requirements and will continue to monitor this space for further developments.