LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Uncertainties In Cloud Security Update May Deter Contractors

By **Daniel Wilson**

Law360 (November 2, 2023, 6:50 PM EDT) -- A long-awaited update to federal cybersecurity standards for cloud computing providers is likely to attract new contractors to work with the government, but uncertainties about exactly how proposed changes will be implemented could limit the effectiveness of the overhaul.

The Office of Management and Budget last week introduced a draft update to its implementation guidance for the Federal Risk and Authorization Management Program, or FedRAMP, a mandatory program for cloud services used by federal agencies that sets out authorization, security and continuous monitoring requirements. Driven by the program finally being formally authorized in the 2023 National Defense Authorization Act, it is the first update to that guidance since the program was introduced in 2011.

The proposed changes address OMB's concern that the current FedRAMP marketplace, with about 300 cloud services available, is unable to meet all the cloud-related needs of federal agencies and the updated guidance memorandum is intended to recognize changes in the types of services available through the cloud and "rapidly increase" the size of the marketplace, OMB said.

However, the guidance is silent on issues such as whether the FedRAMP program management office will be given additional resources to support its expanded role and when federal agencies may refuse to recognize other agencies' authorizations.

"There's certainly lots of areas [in the guidance] where they've noted it's left up to agencies to work on [and] this is a formative time for the FedRAMP program, so industry will need to ensure that they submit comments," said Stacy Hadeka, counsel at Hogan Lovells who advises clients on cybersecurity requirements.

For example, OMB has created new ways for cloud contractors to secure FedRAMP authorization for their products, such as joint-agency authorizations where multiple agencies can work together on an authorization application, and allowing the FedRAMP Program Management Office, or PMO, to conduct authorizations itself.

Currently, authorization can only be granted by a specific agency that needs a cloud service or by using one of the very limited "provisional" authorization slots offered by the FedRAMP Joint Authorization Board, a decision-making body for the FedRAMP program that includes representatives from several agencies.

The new pathways are intended to help speed up new authorization applications and address an authorization backlog which has taken months and sometimes years for new cloud services to get approved, said Morrison & Foerster LLP government contracts and public procurement practice co-chair Tina Reynolds.

"We have clients that have taken 18, 24 months to get authorization," she said. "And not because there's a problem with their product or anything like that, but just because it sits awaiting authorization for a really long time."

But the draft memo provides little information about what the proposed PMO authorization process will look like or if that office will get additional money or staff to support its new role.

"Whether or not [that] office has the resources to be able to roll out a lot of authorizations on its own will remain to be seen," said Sheppard Mullin Richter & Hampton LLP partner Townsend Bourne, who specializes in cybersecurity and data protection issues for government contractors.

Similarly, the draft introduces a "presumption of adequacy," meaning a FedRAMP authorization granted for a cloud product by one agency will now be presumed to carry through to other agencies, another potential avenue for speeding up the authorization process and reducing the backlog.

"Allowing a single agency to do the authorization and have that adopted by others just makes sense," Reynolds said. "There's no reason that multiple agencies have to review the same information and confirm that the product is safe to be used for their agency — if one has already done it, that would be acceptable."

But reciprocity isn't guaranteed and agencies can still determine that they require security controls for a cloud service beyond what is in another agency's existing authorization. Agencies with unique security needs can reject other agencies' authorizations if they have a "demonstrable need," a standard not specified in the guidance.

That lack of guaranteed reciprocity could limit the benefits of the "presumption of adequacy," and agencies could even create their own rules, according to Hogan Lovells' Hadeka.

"Companies will certainly hope that that won't happen and that they can rely just on one [authorization to operate]," she said.

Another area of ambiguity is where the draft guidance supports increased automation for FedRAMP authorization and monitoring. According to Reynolds, it's unclear whether applicants in the middle of the authorization process will be able to amend their applications to take that change into account, or if they would have to "start the process over."

More broadly, the memo does not address how cloud contractors should respond to potential clashes between those updated FedRAMP requirements and other federal cybersecurity requirements.

With the draft guidance open to comment until Nov. 27, and comment on related pending Federal Acquisition Regulation cybersecurity rules open until Feb. 2, cloud service providers should weigh in during those comment processes to try to get the government to "connect the dots between the two," Hadeka said.

If OMB can clear up those uncertainties, the concept of a more streamlined, consistent and quicker FedRAMP authorization process that reflects the current state of the cloud market as outlined in the draft memo should make participation in the FedRAMP marketplace more attractive to cloud service providers, according to Hadeka.

"That's certainly the hope," she said. "I do think industry welcomes these changes, and is certainly going to take advantage of the new consistencies [and] making things more simple — it should remove some of those barriers to entry."

--Editing by Kelly Duncan.
