U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Via email: www.regulations.gov

December 22, 2023

Clare Martorana
Federal Chief Information Officer
Office of Management and Budget
1650 Pennsylvania Avenue, NW
Washington, DC 20502

Re: Request for Comments on Updated Guidance for Modernizing the Federal Risk Authorization Management Program (FedRAMP); *Federal Register*, October 27, 2023; Docket # OMB–2023–0021

Dear Ms. Martorana:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Office of Management and Budget's (OMB's) draft memorandum on modernizing FedRAMP (the draft memo). We also appreciate the additional time that was given to stakeholders to provide officials with substantive feedback.[1]

The Chamber's membership includes numerous federal contractors and cloud service providers (CSPs) that partner with federal agencies and operate within the FedRAMP structure. In general, the Chamber supports the FedRAMP model and considers it a constructive tool for CSPs to deliver innovative and secure cloud products and services to the federal government. However, we believe there are critical aspects of the present FedRAMP model that hinder the commercial sector's ability to work with agencies in the most productive and efficient manner.

The Chamber believes that it is important for OMB to modernize FedRAMP. We are providing this letter to highlight approaches that should reduce complexity and promote modern commercial cloud solutions for the government. We do not address all elements of the draft memo.

Our comments are organized into the following five sections:

[1] https://www.federalregister.gov/documents/2023/10/27/2023-23839/request-for-comments-on-updated-guidance-for-modernizing-the-federal-risk-authorization-management
https://www.federalregister.gov/documents/2023/11/20/2023-25594/request-for-comments-on-updated-guidance-for-modernizing-the-federal-risk-authorization-management

1. Strengthen FedRAMP by adapting to today's commercial cloud environment.

2. Increase the commercial cloud solutions and prioritize reciprocity among authorizations.

3. Harmonize agency requirements to improve cybersecurity and cost efficiencies.

4. Ensure a fair and transparent transition to the new FedRAMP policy structure.

5. Manage the implementation of the updated FedRAMP structure with input from industry.

1. Strengthen FedRAMP by adapting to today's commercial cloud environment.

OMB's draft memo states that the purpose of FedRAMP is to increase federal agencies' adoption and secure use of the commercial cloud, while focusing cloud service providers and agencies on the highest-value work and eliminating redundancy.[2] The Chamber believes that promoting the use of commercial cloud offerings within the federal government would improve service delivery to the government as a whole, particularly as it relates to mission-related metrics, performance, and security.

A business told the Chamber, "This switch emphasizes what is arguably the main benefit—that is, moving away from a government-centric cloud to one that emphasizes the cutting-edge features of commercial clouds. As a result, true hyperscale compute capabilities should become more readily available to the public sector." The business added, "The relative handfuls of government-centric data centers not only lack parity with commercial cloud offerings, but they may never provide enough compute power to manage AI, quantum, and cloud high-performance computing."

Further, a core mission of FedRAMP is to provide federal agencies with a standardized and streamlined process through which they may utilize a wide array of secure and optimized commercial cloud products.[3] The draft memo recognizes that the government "benefits most from the investment, security, maintenance, and rapid feature development that commercial cloud providers must give to their core products to succeed in the marketplace."[4] Similarly, the draft memo notes that FedRAMP is "a bridge" between industry and the government and

[2] OMB draft memo, "Modernizing the Federal Risk Authorization Management Program (FedRAMP)," October 27, 2023, p. 3.
https://www.cio.gov/assets/files/resources/FedRAMP-updated-draft-guidance-2023.pdf
https://www.whitehouse.gov/omb/briefing-room/2023/10/27/office-of-management-and-budget-releases-draft-memorandum-for-modernizing-the-federal-risk-and-authorization-management-program-fedramp

[3] Draft memo, p. 3.

[4] Draft memo, p. 4.

is “expected to thoughtfully navigate situations where unthinking adherence” to rote agency practices in a commercial environment “could lead to unexpected or undesirable security outcomes.”[5]

Such an approach should enable agencies to better leverage best practices, economies of scale, and innovation that characterize commercial cloud environments rather than government-centric cloud products. The Chamber contends that increasing the adoption of private cloud offerings would be crucial in creating cost-effective, modern, and resilient computing capabilities for federal entities.

2. Increase the commercial cloud solutions and prioritize reciprocity among authorizations.

Policymakers are seeking to rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures.[6] In 2022, Congress passed the FedRAMP Authorization Act, featuring language often referred to as the “presumption of adequacy” provision.[7] This section of the law calls for reducing the duplication of security assessments and other obstacles to agency adoption of cloud solutions by establishing a presumption of adequacy for cloud technologies that have received FedRAMP certification.[8] The statutory presumption of adequacy is necessary for agencies seeking to fulfill FedRAMP’s purpose of reusing FedRAMP authorizations.

It is constructive that the White House called for increasing the quantity of commercial cloud products and services receiving FedRAMP authorizations by “bringing agencies together to evaluate the security of cloud offerings and strongly incentivizing reuse of one FedRAMP authorization by multiple agencies.”[9] What this means in practice is that the four proposed FedRAMP authorizations—a single agency authorization, a joint agency authorization, a program authorization, and any other type of authorization—come with a

[5] Draft memo, p. 3.

[6] Draft memo, pp. 3–4.

[7] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (P.L. 117-263), 136 STAT. 3454.
https://www.congress.gov/bill/117th-congress/house-bill/7776/text

[8] “Connolly, Comer, Peters, Portman Applaud House Passage of FedRAMP Authorization Act in FY23 NDAA,” December 8, 2022.
https://connolly.house.gov/news/documentsingle.aspx?DocumentID=4662

[9] The White House and OMB, “Office of Management and Budget Releases Draft Memorandum for Modernizing the Federal Risk and Authorization Management Program (FedRAMP), October 27, 2023.
https://www.whitehouse.gov/omb/briefing-room/2023/10/27/office-of-management-and-budget-releases-draft-memorandum-for-modernizing-the-federal-risk-and-authorization-management-program-fedramp

presumption of adequacy to promote “reusability while accommodating different use cases within the federal government.”[10]

By emphasizing agencies’ use of existing authorizations—effectively enabling reciprocity—FedRAMP should help ensure that agencies can quickly adopt commercial cloud solutions and facilitate the use of emerging or leading technologies that would otherwise be absent from the federal cloud environment.

The Chamber appreciates the draft memo’s recognition that “[M]any existing cloud offerings have implemented or received certifications for external security frameworks. Performing an assessment of such a framework each time a product that uses it goes through the FedRAMP process unnecessarily slows the adoption of such cloud products and services by the Federal Government.”

In addition, OMB writes, “FedRAMP will establish standards for accepting external cloud security frameworks and certifications, based on its assessment of relevant risks and the needs of Federal agencies. This will include leveraging external security control assessments and evaluations in lieu of newly performed assessments, as well as designating certifications that can serve as a full FedRAMP authorization, especially for lower-risk products and services.”[11]

3. Harmonize agency requirements to improve cybersecurity and cost efficiencies.

OMB’s modernization efforts seem to be a productive step toward improving federal cybersecurity and leveraging the commercial cloud marketplace. At the same time, it is essential that officials take tangible steps toward harmonizing FedRAMP rules with related programs. Harmonization needs to occur both within FedRAMP and the federal contracting space in general. A company told the Chamber that “OMB should view its efforts to modernize FedRAMP as an opportunity to promote better policy alignment across the federal government as it relates to the regulation of CSPs.”

What’s more, “Government contractors, CSPs, and other operators of federal information systems frequently find themselves on the receiving end of myriad different requests for information, patching mandates, and disclosure requirements that hamper their ability to effectively provide the government with secure and technically sound cloud service,” the company said.

For example, CSPs that work with the Cybersecurity and Infrastructure Security Agency (CISA) are often subject to various binding operational directives (BODs) and emergency directives (EDs) that, while important, could impact a CSP’s ability to adhere to FedRAMP frameworks and seamlessly partner with the government. OMB should consider weaving BODs, EDs, and related requirements into FedRAMP’s future compliance

[10] Draft memo, pp. 6–7.

[11] Draft memo. p. 10.

mechanisms, rather than stipulate compliance with additional rules and workflows that are not aligned with FedRAMP.

In addition, from the perspective of many businesses, the perceived aims of FedRAMP modernization remain at odds with the intent of existing efforts to amend certain procurement rules. To illustrate, a proposed rule (FAR case 2021-019) pertaining to Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, appears to take a comparatively rigid approach to contract compliance, including focusing on specific cybersecurity controls. The proposed rule—issued by the Department of Defense (DoD), the General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA)—seems to conflict with the purpose of OMB's draft memo, which emphasizes flexibility, risk acceptance, and adaptiveness.

OMB plays a crucial role in managing both the proposed rule and FedRAMP modernization. Knowing this, stakeholders would benefit from having OMB ensure that its Office of Federal Procurement Policy (OFPP) and Office of the Federal Chief Information Officer (OFCIO) harmonize the requirements between the proposed rule and FedRAMP—particularly in areas where existing compliance mechanisms in FedRAMP can lead to reciprocity between proposed FAR rules and the evolving FedRAMP process.

Furthermore, an organization said to the Chamber, "OMB needs to understand that the federal government is not the sole public sector customer for commercial cloud service providers and should consider how updating FedRAMP could impact the commercial sector's existing partnerships." The organization added, "All U.S. states have apparently granted reciprocity for products certified in the FedRAMP marketplace. However, this is not guaranteed. The federal government should take steps to prevent fragmentation among the states and relevant state agencies to drive adoption with either FedRAMP authorized products or NIST Special Publication 800-53 security controls."[12]

In sum, OMB's FedRAMP modernization effort provides an ideal way for OMB to drive regulatory harmonization across key parts of the federal IT ecosystem. As the government updates FedRAMP, officials need to contemplate how the proposed changes interact with other cybersecurity requirements of similarly situated programs. Doing so should increase efficiency, consistency, and resilience across commercial digital products utilized by multiple agencies.

4. Ensure a fair and transparent transition to the new FedRAMP policy structure.

The draft memo outlines a series of ambitious timelines within which OMB and other relevant federal entities must implement a broad array of modernization directives. First, the draft memo calls on agencies to issue or update agencywide policy that aligns with the requirements of the draft memo within 180 days of the issuance of the draft memo. And within the same time frame, FedRAMP must update its continuous monitoring process guidance and associated documentation.

[12] https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

Within one year of the issuance of the draft memo, GSA must provide a plan to structure FedRAMP to encourage the transition of agencies away from the use of government-specific cloud infrastructure. Despite or because of the numerous timelines, there remains a lack of clarity among business entities about when the transition to the new authorization structures from the traditional FedRAMP Joint Authorization Board provisional authority to operate—aka the JAB P-ATO—framework would occur.

In light of this situation, a business said to the Chamber, "OMB should allow for additional transition time, such as one year, for this policy to take effect." The business added, "Doing so would provide clarity to CSPs and allow for businesses to adjust internal processes to facilitate FedRAMP's transition."

Similarly, a company expressed concern that the transition period could negatively affect authorizations currently under consideration by the JAB. This concern is echoed in the draft memo's implementation section where OMB requires GSA to submit a plan that would "include a timeline and strategy to bring any pending authorizations or existing FedRAMP initiatives into conformance with the Authorization Act and this memorandum."[13] The company told the Chamber, "It is critical that pending authorizations are not negatively impacted by the transition. We want to ensure that these products are given full and fair consideration as part of the JAB process before a transition takes place, including that OMB gives assurances in its guidance that the timeline to approve such products would not be delayed." The company added, "Industry wants to deliver a range of cloud products and services, including innovative AI tools, to the government with confidence and without disruption."

One firm said, "While due diligence and generally avoiding disruptions are critical, we would still like to stress the necessity of speed as it relates to modernizing federal IT infrastructure. FedRAMP needs to evolve to meet the shift away from legacy, on-premises computing infrastructure, and government-centric clouds. It must be ready and capable of evolving at an equally fast rate. Doing so would ensure that the government has access to the latest security, technology, and related features."

Second, in order to realize the benefits of new authorization structures, the government needs to distinguish the emerging multiple authorization structure from the prior FedRAMP policy structure. OMB should consider and make known how a multiple authorization structure would differ from the current JAB authorization model, which OMB is moving away from.

OMB is urged to address the following issues and questions:

- How would the change in agency authorizations impact CSPs that have made, including at the time of this writing, significant investments in JAB authorizations?

[13] Draft memo, p. 17.

- How would OMB and GSA monitor consistency across joint agency annual assessment, authorization timing, and boundary guidance rules? (The draft memo notes, “Existing JAB P-ATOs at the time of the issuance of this memorandum will be automatically designated as joint agency FedRAMP authorizations.)[14]

- How would FedRAMP (e.g., from perspectives regarding technical controls and continuous monitoring) reduce the time required for achieving and maintaining an authorization by the joint agency process given that there may be new agencies participating in the program?

- How would OMB and GSA ensure that the goal of increased authorizations is met when authorizing officials are new to the program and may have lengthy learning curves?

5. Manage the implementation of the updated FedRAMP structure with input from industry.

Once FedRAMP’s proposed multiple authorization framework is established and functioning, it is key that DoD, the Department of Homeland Security (DHS), and GSA continue to collaborate on cloud security authorization processes as they have over the past decade with a JAB P-ATO. Doing so would promote consistency across the authorization and annual assessment processes and enable companies to serve agencies more efficiently.

A company said to the Chamber, “For CSPs engaging in work across both civilian and DoD agencies, a JAB authorization was a prerequisite for obtaining DoD Impact Level IL 5 authorizations. We recommend that OMB consider the impact of the dissolution of the JAB structure and its impact on prior collaborations between the FedRAMP Project Management Office (PMO) and the Defense Information Systems Agency (DISA) Risk Management Executive (RME).” The company recommended that “GSA and OMB should work with DoD and DISA’s RME and authorizing official to enable continued commercial cloud adoption across government.

Moreover, the firm told the Chamber, “DoD should be invited to participate in the joint agency authorization paradigm. DoD should engage as a policymaking partner on the FedRAMP board to ensure that there is continued regulatory harmonization across IT risk management frameworks inside the government.”

A key aspect of FedRAMP’s proposed multiple authorization structures is its PMO. The Chamber believes that creating a new avenue for authorizations through the FedRAMP PMO is a positive development. As the draft memo states, the FedRAMP PMO “oversees the process for all FedRAMP authorizations, and works with agency program staff and authorizing officials to make necessary risk management decisions.”[15]

[14] Draft memo, p. 7.

[15] Draft memo, p. 7.

An organization told the Chamber, “As the PMO is established and its purview expands, appropriate resources and clear direction are going to be critical to its success. The PMO could very quickly be overburdened with new authorizations as well as pending authorizations from CSPs that have not acquired an agency sponsor.” The organization added, “OMB and other policymakers should provide adequate resourcing for the PMO and consider methods to get CSPs across the finish line in an equitable and timely manner.”

Separately, a firm noted, “We are open to suggestions from others on how to accomplish these goals, but other than in the event of an emergency or other extraordinary event, a first-in, first-out approach seems fairer than assessments based on the impact level or prioritizing CSPs that already have authorizations.”[16] Furthermore, “As the PMO reviews authorizations and works with agencies to make necessary risk management decisions, it is critical that the PMO appreciates the varying degrees to which a vulnerability may pose risks to the integrity of a cloud service product,” the firm said. “Doing so would increase transparency for CSPs and improve the efficiency of FedRAMP as a whole.”

The draft memo indicates that when the FedRAMP PMO becomes aware of vulnerabilities in a CSP with a FedRAMP authorization, it would provide that information to the CSP and “establish escalation pathways for vulnerabilities not sufficiently addressed in a timely manner. Escalation pathways may include public notification of unaddressed concerns for potential agency customers.”[17]

In addressing these issues with CSPs, OMB should consider viewing discovered vulnerabilities through a risk-based lens and focus its efforts and resources on the most exploitable vulnerabilities.[18] A company expanded on this concept, saying, “While there are many ways for a PMO to gain knowledge of an alleged vulnerability, not all reporting channels can be trusted to be accurate. Some reports may be malicious. Running down false positives can be a huge waste of security professionals’ time and resources.”

Overall, the establishment of a multiple authorization structure is a welcome development for CSPs wanting to work with the government. “Among other things, it serves as an acknowledgment from OMB that software-as-a-service (SaaS) products and services, which are cloud-based applications made available over the internet, could one day support critical aspects of an agency’s mission,” one industry entity said to the Chamber.

[16] The firm explained, “Arguably, there are times of emergency where we would want some types of applications prioritized. COVID-19 required remote and hybrid work tools and associated updates to cut the line. The administration has floated the idea of having AI tools do the same. We could see cybersecurity or disaster recovery tools being subject to the same need in a major emergency.”

[17] Draft memo, p. 12.

[18] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

However, there are additional procedures that OMB should consider that could further improve the efficiency of a multiple authorization structure:

- The draft memo says that FedRAMP expects to "update its security baselines to align with a threat-based analysis, produced in collaboration with [CISA], that focuses on the application of those controls that address the most salient threats."[19] A private entity told the Chamber that this topic "needs further clarification by OMB. How can we ensure that contractors can keep up with the pace of updates to the security baselines?"

- In order to provide quicker and more effective adoption of these new authorizations, OMB should explore the establishment of mechanisms that keep CSPs continually apprised of new opportunities and policy developments so that they can more effectively navigate the new authorization processes.

- OMB should clarify its policy goals so that if a service is FedRAMP authorized, it should not need a plan of action and milestones (aka a POA&M) in order for it to be used in a subsequent FedRAMP-authorized system.

- The government needs to consider reconciling its desire for efficiency and consistency within FedRAMP with the fact that certain federal security standards and guidelines have not kept pace with commercial sector innovation.

  For example, a business told the Chamber, "Validation of new cryptographic modules under the Federal Information Processing Standard program (FIPS) has lagged behind private sector best practices for years. This has caused a bifurcation between innovative commercial solutions and those sold to government agencies. FIPS has not kept pace with innovations, and its lack of approvals for cryptographic modules meaningfully impacts federal cybersecurity."

  The business added, "OMB should consider the drawbacks of the current FIPS and proactively instruct GSA and joint agency authorizers on the specific interpretation of FIPS that would yield the most flexibility in FedRAMP. It is important that federal IT systems are not subject to additional risk because they are using outdated and insecure cryptographic modules for the sake of compliance."

***

Thank you for the opportunity to provide comments on modernizing FedRAMP. If you have any questions or need more information, please do not hesitate to contact Jack Overstreet (joverstreet@uschamber.com) or Matthew Eggers (meggers@uschamber.com).

[19] Draft memo, p. 8.

Sincerely,

Jack Overstreet
Director
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Matthew J Eggers

Matthew J. Eggers
Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce