FEDERAL SECURE CLOUD
ADVISORY COMMITTEE

fscac@gsa.gov
gsa.gov/fscac

November 20, 2023

Robin Carnahan
GSA Administrator

Ann Lewis
FSCAC Chair

Federal Secure Cloud Advisory Committee (FSCAC) Feedback to the GSA Administrator on the 2023 Draft Office of Management and Budget (OMB) Memo, "Modernizing the Federal Risk Authorization Management Program (FedRAMP)"

Background & Summary

The Federal Secure Cloud Advisory Committee (FSCAC) has been requested by the GSA Administrator to review the draft OMB Memo titled, "Modernizing the Federal Risk Authorization Management Program (FedRAMP)," and provide formal committee feedback. After careful deliberation, the Committee would like to present the following feedback on the draft OMB Memo titled, "Modernizing the Federal Risk Authorization Management Program (FedRAMP)." This Committee finds the memo, although thorough and detailed, lacking clarity and specificity in some key areas, specifically section IV. The FedRAMP Authorization Process, section VI. Continuous Monitoring, and section VII. Roles and Responsibilities.

Overall, the FSCAC identified the following general areas of feedback:

- Standards/Process Changes
  - Inconsistency with NIST standards
  - Advocating risk acceptance authority of the FedRAMP
  - Requesting reciprocity with other security certification programs
  - Removal of FedRAMP as mandatory for the Federal acquisition of cloud services by rescinding previous OMB memo
- Small Business
  - Failure to address small businesses
- Budget
  - Increase in compliance cost to Federal agencies
- Potential Benefits
  - Removing incentives for separate commercial and government cloud instances promises cost savings for government and industry

Cordially,

Ann Lewis
FSCAC Chair

fscac@gsa.gov
gsa.gov/fscac

Appendix A: Compilation of FSCAC Feedback

Feedback is organized by the section of the draft OMB memo. All direct quotes from the draft OMB memo are italicized.

I. Background

-
-
-
-

II. Vision

- *"FedRAMP should not incentivize or require commercial cloud providers to create separate, dedicated infrastructure for Federal use, whether through its application of Federal security frameworks or other program operations." (page 4)*
    - Any step to allow for a mix of government and commercial customers when dealing with Moderate or lower impact levels would be a huge savings for many CSPs.
- *"The FedRAMP Board, composed of Federal technology leaders appointed by OMB, …" (page 4)*
    - It is important to ensure this board contains small business representatives. There are a large number of small business CSPs that can provide valuable services to the government. The incredible cost of FedRAMP is a barrier to entry. There have been multiple public comments to FSCAC regarding small businesses being negatively affected by cost and resource requirements.The committee recommends costs remain as low as possible both in money and in resources to support small business concerns.
- *"Leverage shared infrastructure between the Federal Government and private sector." (page 4)*
    - This can have potential impact on the NIST Cybersecurity RMF which mainly focuses on securing Federal Information systems. The framework will have to be updated to reflect this change.
- *"Rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures." (page 3)*
    - This requirement translates to an increased operational impact to all federal agencies.
- *"Streamlining processes through automation." (page 4)*

- Significant challenge to identify, implement and support an Enterprise solution across the federal workspace.

III. Scope of FedRAMP

- *"Those products and services are: (1) commercially offered cloud products and services (such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service) that host information systems that are operated by an agency, or on behalf of an agency by a contractor or other organization." (page 4)*
  - These products and services (IaaS, PaaS, SaaS) are more complex/diverse, requiring a broader support base (skill set base) for our Cloud Support Team (CST) than the originally focused FedRAMP memo that initially looked at IaaS only 10 years ago.
- *"Cross-Government shared services…" (page 4)*
  - There are no current documented requirements for a CSP to be defined as a Cross-Government shared service.
- *"Publicly available social media or communications platforms governed under Federal agency social media policies, in which Federal employees or support contractors may or may not enter Federal information." (page 5)*
  - This is a potential risk and should be considered to be in FedRAMP's scope.

IV. The FedRAMP Authorization Process

- "*To that end, if a given cloud product or service has a FedRAMP authorization of any kind, the Act requires that agencies must presume the security assessment documented in the authorization package is adequate for their use in issuing an authorization to operate, and that* ***neither additional security controls*** *nor additional assessments of those controls are required."* (page 5) (Emphasis added)
  - This statement is factually incorrect. The FedRAMP authorization only covers roughly 2/3 of the controls listed by NIST and required by FISMA to issue an ATO. The other third are part of the baseline that the agency is responsible for evaluating. Moreover, 44 U.S.C. § 3613(e)(1) only states that those controls as assessed as part of the authorization are sufficient for agency acceptance, and not that those controls are the only ones needed to issue an ATO. Please refer to NIST 800-53B rev 5, Chapter 3 for the full list of controls required by impact level, and compare to FedRAMP's security controls baseline.
    - https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final

        - https://www.fedramp.gov/baselines/
        - Recommend to update this language to make it clear that other controls are indeed needed for an ATO and required by law.
- *"A joint-agency authorization…" (page 7)*
    - One of the painful starts to the FedRAMP program is finding a sponsor for FedRAMP ATOs. If two or more agencies can share in the responsibility, it may make things easier to find and secure a sponsor.
- *"A program authorization…" (page 7)*
    - As mentioned above, finding a sponsor can be difficult and can lead to delays of providing services to the government. StateRAMP has this process already where a sponsor is not needed, nor is the intense process of the legacy JAB. There are many CSPs that have CSOs that would benefit the government, but there is a trust issue with agencies having to use a FedRAMP solution, but the FedRAMP solution can't exist until an agency uses it.
- *"The authorization process must integrate agile principles…" (page 8)*
    - This was discussed heavily in the FSCAC meetings where FedRAMP is not agile enough, especially for SaaS solutions. Heavy focus should be put into prioritizing specific controls and/or other risk items that have surfaced. While the list of core controls for an annual assessment is useful, other factors should be in place that would be based on the current risk environment.
    - In response to the authorization process improvements and their need to be agile on page 8, currently FedRAMP is heavy on documentation, and the assumption is that all (let's say) FIPS 199 moderate classified systems are like all other FIPS 199 moderate classified systems and thus require the same paperwork, and perhaps a more risk-based baseline approach rather than the generation of documentation as the baseline would be more efficient as well as more secure.
- *"The FedRAMP PMO is responsible for ensuring that the types of authorizations described above successfully achieve their goals, and for generally enabling Federal agencies to safely meet their mission needs. 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." (page 7)*
    - It is not explicitly clear that the preceding authorization types still have to ultimately undergo FedRAMP authorization issued by PMO separate from any agency authorization, joint agency authorization, etc.
        - Recommendation: State that despite the expansion of the authorization types, FedRAMP authorization by the PMO is still required in addition to any agency authorization granted (where required per the authorization type).

- *"Agency authorizing officials determine acceptable risk for their agency, and the FedRAMP Director determines acceptable risk for what can be called a FedRAMP authorization." (page 7)*
    - Historically speaking the PMO has repeatedly stated that they "cannot accept risk," and this statement is in conflict with that. The program authorization path is also in conflict with this.
        - Recommendation: FedRAMP PMO must be allowed to accept risk, and this must be documented as a responsibility. This will be particularly important in the context of a program authorization. Else, the PMO will default to zero risk, and that is unattainable in FedRAMP with the stringent requirements.
- *"The FedRAMP Director should draw on technical expertise across government and industry as necessary to ensure that appropriate teams can conduct these assessments." (page 8)*
    - "Appropriate teams to conduct assessments" is misleading since largely accredited 3PAOs perform this work.
        - Recommendation: Clarify that assessments are performed by 3PAOs. Historically speaking, JAB and some agencies required accredited 3PAOs, but some did not. Since the primary concern of PMO is quality issues, requiring formal 3PAOs would do some to relieve these concerns.
- *"The FedRAMP Program will update its security baselines to align with a threat-based analysis, produced in collaboration with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), that focuses on the application of those controls that address the most salient threats." (page 8)*
    - While active technical controls are important, there is still a need for things like documentation and backup testing and other controls that may not be at the top of the list for what CISA has determined to be the most salient threats, but there is still merit for these controls to be implemented by CSPs and integrated into the lifecycle.
        - Recommend that more guidance be issued here or guidelines or expectations to ensure that the overall security of the system not be reduced/compromised. FedRAMP baselines are based on FISMA and tailored from there.
- *"GSA, in consultation with the FedRAMP Board and the Chief Information Officers Council, develops criteria for prioritizing products and services expected to receive a FedRAMP authorization.[1] GSA will ensure that these criteria prioritize products and services based on agency demand, and critical technologies that might otherwise remain unavailable to agencies, while facilitating the goals of this policy, such as automation, shared commercial platforms, and reuse." (page 9)*

[1] 44 U.S.C. § 3609(b)(2).

    - What purpose does prioritization serve and how does it impact the authorization types? How will it be enforced among CSPs and 3PAOs?
        - Recommendation: More clarity needs to be provided here.
- *"To identify more cloud services that could become FedRAMP authorized, and to accelerate their eventual path to being authorized, FedRAMP will provide additional procedures for the issuance of a type of preliminary authorization that would allowFederal agencies to pilot the use of new cloud services that do not yet have a full FedRAMP authorization. Consistent with FedRAMP's policies and procedures, such a preliminary authorization would provide for use of the covered product or service on a trial basis for a limited period of time, not to exceed twelve months, with the goal of more easily supporting a potential FedRAMP authorization." (page 9)*
    - A preliminary authorization is another authorization type.
        - Recommendation: This should also be addressed on page 7 with the list of other authorization types.
    - The point of this sounds very similar to the existing FedRAMP Ready process.
        - Recommend building on the existing FedRAMP Ready process to formalize the preliminary authorization. Recommend that FedRAMP elevate the increasingly demanding and stringent FedRAMP Ready process to the Preliminary Authorization, then revamp the Ready process back to its original intent.
- *Single-agency authorization: "The FedRAMP Director is responsible for ensuring that the authorization can reasonably support reuse by agencies with similar needs." (page 6)*
    - This statement conflicts with the purpose of this type of authorization. It appears to go through the same review and approval as it does today for agency sponsored CSPs. It seems redundant to review again once an agency authorizes the CSP.
- *Joint-agency authorization: "signed by two or more Federal agencies' authorizing officials, that indicates that the agencies assessed a cloud service's security posture and found it acceptable." (page 7)*
    - The process for an agency identifying another agency interested in the same CSP is not defined. There needs to be a means for the agencies to know this level of interest. Other agencies that will be utilizing the JA authorization will still need to issue an agency ATO.
    - The addition of FedRAMPs ability to support multiple ATO types discussed on pages 6 and 7 (i.e. a joint agency authorization) should open the door for agencies to use FedRAMP more effectively, such as improving reciprocity.
    -

- *"A program authorization, signed by the FedRAMP Director, that indicates that the Program assessed a cloud service's security posture and found it met FedRAMP requirements and is acceptable for re-use by agency authorizing officials." (page 7)*
    - This type of authorization should be signed by the FedRAMP Board instead of the director before use. It's not clear what is meant by "…acceptable for re-use by agency authorizing officials."
- *"FedRAMP reviews are not limited to reviewing documentation, and may direct that intensive, expert-led "red team." (page 7)*
    - Clear direction must be documented: who leads the "red team," the agency or the PMO?
- *"To identify more cloud services that could become FedRAMP authorized, and to accelerate their eventual path to being authorized, FedRAMP will provide additional procedures for the issuance of a type of preliminary authorization that would allow Federal agencies to pilot the use of new cloud services that do not yet have a full FedRAMP authorization." (page 9)*
    - The type of data used (federal or dummy) needs to be defined prior to the pilot.
- Page 5, overall
    - Need a process for expediting FR ATO reviews at the PMO - suggest mandatory RAR for any new CSP (i.e. one that doesn't already have a FR offering) coming into the process, or potentially for CSPs working with a new agency that has never sponsored a CSP before.
    - Need better communications from PMO wrt package progress, updates, etc.
    - Need a minimum risk posture for agencies to adhere to (i.e. some risks are accepted, others must be fixed prior to ATO) so that all agencies and CSPs know the minimum bar
- *"This presumption of the adequacy of FedRAMP authorizations does not supersede or conflict with the authorities and responsibilities of agency heads under FISMA to make determinations about their security needs. An agency may overcome this presumption if the agency determines that it has a "demonstrable need" for security requirements beyond those reflected in the FedRAMP authorization package,[2] or that the information in the existing package is "wholly or substantially deficient for the purposes of performing an authorization" of a given product or service.[3] The FedRAMP Director remains responsible for deciding whether an agency's additional security needs merit devoting additional FedRAMP resources and conducting additional FedRAMP authorization work to support a revised package. If additional authorization work is conducted and a new authorization is issued, the sponsoring agency must also document in the resulting authorization package the reasons that it found the existing*

[2] *Id.* § 3613(e)(2)(B).
[3] *Id.* § 3613(b).

FedRAMP package deficient. However, these instances should be uncommon, in keeping with this policy of presuming the adequacy of FedRAMP authorizations." (page 5-6)

- It would be helpful to provide criteria in how the FedRAMP board and/or Director determines if a package may require additional work.

V. Automation and Efficiency

- *"Additionally, many existing cloud offerings have implemented or received certifications for external security frameworks." (page 10)*
  - It would be beneficial to have reciprocity with other certifications. StateRAMP has taken this approach with HITRUST in that having one can allow for reciprocity on the other. If having FedRAMP also gets you 90% of the way to other compliance programs, more CSPs will be willing to go through the FedRAMP process. They will receive a bigger return on investment if having FedRAMP also gets them 90% of the way to PCI, SOC 2, ISO 27001, etc.
- *"To accelerate the adoption of secure cloud computing products and services, FedRAMP must maintain an analysis of what controls can be shared between cloud products and services that rely on an underlying platform or infrastructure offering. FedRAMP will use that analysis to create guidance that streamlines authorizations for cloud services that use FedRAMP authorized infrastructure or platforms." (page 10)*
  - Recommend that in addition to the CIS and CRM that a successful package be required to include a configuration guide for any customer configurations that must be made in the CSO to ensure full compliance. Note that some customer responsibilities will be not configurable within the CSO and will remain a customer responsibility of the CSP outside the CSO.
- *"Therefore, 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. FedRAMP may make risk management decisions regarding acceptable controls for certain situations or types of cloud offerings where there are gaps or misalignments between Federal and external security frameworks, weighing whether broader interoperability with industry security processes, reduced burden on providers, or further streamlining of FedRAMP authorizations and processes may justify acceptance of a given level of security risk any." (page 10)*

- FedRAMP exists because no other framework meets the intent nor the requirements. There is no other framework that focuses on a cloud service offering boundary like FedRAMP does with the stringency and prescriptiveness that are seen in the controls and FedRAMP-designated parameters.
  - More clarity is required here, and FedRAMP should be instructed to coordinate with 3PAOs and related stakeholders to determine if this order is even feasible. One compromise could be that 3PAOs could be given more flexibility to utilize other assessment evidence and determinations to leverage in FedRAMP assessment testing within a certain rule of thumb. Currently, 3PAOs and CSPs are limited by timeliness of evidence thresholds among general lack of interoperability of FedRAMP's stringent requirements (which is by design).

VI. Continuous Monitoring

- *"Avoids incentivizing the bifurcation of cloud services into commercially-focused and Government-focused instances. In general, to promote both security and agility, Federal agencies should be using the same infrastructure relied on by the rest of CSPs' customer base." (page 11)*
  - Many CSPs make the difficult decision to operate multiple CSOs for dedicated workloads for a variety of reasons – desire to move to IL4 or IL5 that have logical and physical separation for gov-only community clouds, but also because, and most often, commercial customers do not want to be held to the stringent security requirements of FedRAMP. While commercial customers may be fine with certain credential requirements, they may not want the headache and cost of phishing-resistant MFA no matter the gain in security when it's not mandated/required for them. FedRAMP is a significantly higher bar than most.
    - Reconsider the messaging here, particularly any adverse effects for CSPs that still choose to go down the dual offering path as well as any CSPs that currently operate this way. This statement seems somewhat out of touch with the challenges that CSPs face in both the commercial and fed spaces and serving both.
- *"The FedRAMP PMO will set this standard level of monitoring support by analyzing and identifying the highest-impact controls for ensuring security of FedRAMP products and services." (page 11)*
  - The statement is contradictory. If the FedRAMP Board is responsible for setting the requirements and baselines, then it seems logical that they would define the required control selections for annual continuous monitoring assessments.

        - Review roles and responsibilities to ensure they are defined logically between the Board and PMO.
- *"The FedRAMP PMO may conduct a special review of existing FedRAMP authorizations (regardless of authorization type)." (page 11)*
    - Purpose for this review and circumstances in which it would be invoked are unclear.
        - Clarify and provide additional context and purpose.
- *"When the FedRAMP PMO becomes aware of vulnerabilities in a CSP with a FedRAMP authorization, it will provide that information to the CSP and impacted agencies for remediation and establish escalation pathways for vulnerabilities not sufficiently addressed in a timely manner." (page 12)*
    - "Vulnerabilities" is extremely broad and after performing hundreds of FedRAMP Assessments.This type of directive is dangerous without a more clearly defined purpose, boundaries/guardrails, and qualifiers for triggering this process.
        - More bounds are needed for this and more clearly defined instructions and triggers.
- *"The FedRAMP PMO will develop and maintain procedures for responding to CISA Binding Operational and Emergency Directives, in collaboration with CISA, OMB, and the FedRAMP Board." (page 12)*
    - PMO procedures without adequate and timely and consistent dissemination to all stakeholders (CSPs, 3PAOs, etc.) is frankly useless and creates confusion for all stakeholders and additional costs for CSPs. It also leads to many of the quality concerns noted by the PMO.
        - Additional mandates should be issued to FedRAMP PMO to ensure all documentation is updated timely and consistently, and disseminated to stakeholders.
- *"FedRAMP should seek input from CSPs and develop processes that enable CSPs to maintain an agile deployment lifecycle that does not require advance government approval." (page 11)*
    - Advance government approval needs to be defined.
- *"The FedRAMP PMO, in coordination with the Board and CISA, is responsible for establishing a framework for continuous monitoring of cloud services and products." (page 11)*
    - Need to ensure these changes are in compliance with NIST 800-137 Continuous Monitoring Process.
- *"Calls for advance notice from CSPs of upcoming security-relevant changes to the FedRAMP-authorized cloud product or service without requiring advance approval from the Government." (page 11)*
    - Clear definition of "advanced approval" is needed to avoid a potential risk.

- "Avoids incentivizing the bifurcation of cloud services into commercially-focused and Government-focused instances. In general, to promote both security and agility, Federal agencies should be using the same infrastructure relied on by the rest of CSPs' customer base." (page 11)
    - Separation and protection of federal data from commercial data will be key for this to work.
- "Once approved, the FedRAMP Director will work with the FedRAMP Board to jointly convene a technical working group consisting of members from across the Federal Government with relevant expertise." (page 11)
    - Requirements for the technical working group membership needs to be defined.

VII. Roles and Responsibilities

- *"To further strengthen the FedRAMP program, each agency must: 1) Upon issuance of an agency authorization to operate based on a FedRAMP authorization, provide a copy of the authorization-to-operate letter and any relevant supplementary information to the FedRAMP PMO, including configuration information as applicable; 2) Ensure authorization package materials are provided to the FedRAMP PMO using machine-readable and interoperable formats, in accordance with any applicable guidance from the FedRAMP program; 3) Ensure that agency system-inventory tools can ingest machine readable authorization artifacts; 4) Provide data and information concerning how they are meeting relevant security metrics, in accordance with OMB guidance; and 5) Ensure that relevant contracts include the FedRAMP security authorization requirements with which the contractor must comply."* (page 15)
    - This memo is lacking a To: line, Authority, or Definitions section, explicitly listing what agencies this memo applies to. As such, this section creates a very large burden of work on small, non-CFO Act agencies in reporting ATO data back to the FedRAMP PMO – data which in all likelihood will never be used.
        - Recommend amending this to explicitly state only CFO Act agencies are required to comply, in accordance with FITARA and alignment with other similar memos, which typically read: "The requirements in this Memorandum apply to the 24 Federal agencies covered by the Chief Financial Officers (CFO) Act of 1990, including the Department of Defense." (from M-19-19).

- *"Ensure authorization package materials are provided to the FedRAMP PMO using machine-readable and interoperable formats, in accordance with any applicable guidance from the FedRAMP program." (page 15)*
    - o This can only be achieved if the FedRAMP PMO has streamlined automated standards e.g., Open Security Controls Assessment Language (OSCAL).
- *"Provide data and information concerning how they are meeting relevant security metrics, in accordance with OMB guidance." (page 15)*
    - Currently FedRAMP related metrics are reported under metric 1.5: "Report the types of Cloud Services the OpDiv is using by cloud service provider(s) and what service(s) the OpDiv is receiving. (e.g., mail, database, etc.). (NIST SP 800-145)
- "GSA resources, administers, and operates the FedRAMP program office, and is respons*ible for the successful implementation of FedRAMP." (page 12)*
    - I think some Agency training should be an additional responsibility. Many agencies are still lagging behind the top 1% of agencies / JAB / CSPs in terms of understanding FedRAMP and applying the guidance that is provided.
- *"The FedRAMP Board consists of up to seven senior officials or experts from agencies that are appo*inted by OMB in consultation with GSA…" (page 13)
    - Should this section also include "Issue FedRAMP authorizations and conduct Continuous Monitoring" in some capacity? The FedRAMP Board will have the authority to issue authorizations.
- *"To further strengthen the FedRAMP program, each agency must…" (page 15)*
    - Should this section also include "Issue FedRAMP authorizations and conduct Continuous Monitoring" in some capacity? Agencies will have the authority to issue authorizations.
-

VIII. Industry Engagement

-
-
-
-
-

IX. Implementation

- *"Within 180 days of issuance of this memorandum, each agency must issue or update agency-wide policy that aligns with the requirements of this memorandum. This agency policy must promote the use of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance requirements as*

determined by OMB, in consultation with GSA and CISA…. This memorandum rescinds "Security Authorization of Information Systems in Cloud Computing," issued by the Federal Chief Information Officer on December 8, 2011." (page 17)

- By completely rescinding the previous memo but not preserving section 4.d. in this memo, OMB has removed the requirement that agencies must use FedRAMP at all.
  - Recommend that this new memo should restore section 4.d. in its entirety appended to VII.d., including the preservation of 4.d.vii. which provides the critically-needed exception clause, without which many agencies would have been unable to meet their statutory requirements in responding to the COVID-19 pandemic.

X. Rescissions

XI. Policy and Program Implementation Assistance

Additional General Comments

- The concept of the Technical Representatives (GSA, DHS, DOD) that today provide JAB authorizations, continuous monitoring, and change management to the FedRAMP PMO is absent in the draft memo. It is unclear if the FedRAMP Technical Advisory Group or the FedRAMP PMO is going to assume these functions. The manpower and budget required to fulfill the TR role is extensive and not covered today or in the draft memo. This is a glaring gap in the memo and may point to a lack of understanding of the

manpower and budget required by an agency TR. Without a sufficient organizational construct and the appropriate budget, the TR function cannot continue as it exists today.

- Generally the memo was a big step forward and addresses many of the challenges we've been discussing within FSCAC. It provides a clear path for assisting with efforts within federal agencies that can help move SaaS further and smoother, a huge anticipated area of expansion.
- There's also not a clear understanding of SaaS, and many groups are applying "old school" requirements meant for on-prem and/or VAEC to SaaS when it just doesn't make sense to do so. I know this has been discussed many times, but I think it's really important to have quicker, clearer, and more consistent guidance on SaaS, perhaps specifically calling out inappropriate legacy controls that don't make sense for SaaS products.
-
-
-