FEDERAL SECURE CLOUD
ADVISORY COMMITTEE

fscac@gsa.gov
gsa.gov/fscac

MONTH DAY, 202X

Robin Carnahan
U.S. General Services Administration Administrator

Larry Hale
Federal Secure Cloud Advisory Committee Chair

Federal Secure Cloud Advisory Committee (FSCAC)'s 2024 FedRAMP Recommendations to the GSA Administrator

Executive Summary

Recommendations for FSCAC's 2024 Priorities

[Committee Staff will work with Chair to complete the Executive Summary after the recommendations are completed]

Priority 1: Identify and publicly document top challenges and propose solutions around the barrier to entry for CSPs (with a focus on small businesses), 3PAOs, small & large agencies, e.g. ensure minimum risk threshold / minimum acceptability standardized baselines for sponsoring agencies and 3PAOs.

PROBLEM STATEMENT: Small businesses and 3PAOs face significant barriers to entry in the federal cloud market due to complex and costly compliance requirements. These challenges hinder innovation, limit competition, and reduce the diversity of secure cloud solutions available to government agencies. Simplifying these processes and lowering the cost of compliance is essential to fostering a more inclusive, innovative cloud ecosystem.

ACTIONABLE, SPECIFIC RECOMMENDATIONS (with projected benefits):

1. **Reduce the time to authorization by streamlining the existing compliance framework** that applies equally to all CSPs, regardless of size or risk level, by **automating key portions of the compliance process**. This could include automated security controls verification, pre-configured templates, and an **online submission portal** that integrates with existing compliance tools, ensuring faster processing without lowering standards.

    a. The GSA Administrator should recommend that **FedRAMP PMO and the FedRAMP Board Chair** lead the initiative to develop and implement these automation tools, in collaboration with **CSPs** and **technology vendors** who can provide input on efficient compliance mechanisms.

    b. By optimizing the compliance process, **all CSPs—large and small—would face reduced administrative overhead** and time spent on manual documentation, allowing faster time-

to-market for new services. This would encourage broader participation from CSPs without lowering the security bar, improving government access to diverse, innovative solutions while maintaining strong security standards.

2. Create a **centralized technical and compliance assistance program** to provide small CSPs and 3PAOs with **guidance, templates, and resources** to navigate FedRAMP and other security requirements. This could include pre-approved compliance documentation and **access to expert consultation** on meeting federal cloud security standards.

    a. The GSA Administrator should recommend that **GSA's Office of Government-wide Policy (OGP)** and **FedRAMP PMO** establish this program, potentially in collaboration with **industry organizations** (e.g., Cloud Security Alliance, CSP-AB) and **third-party auditors (3PAOs)**, to ensure CSPs have access to the expertise and tools they need.

    b. This program would **reduce the learning curve** for small providers, helping them meet regulatory requirements more quickly and affordably. It would also **increase compliance accuracy** and **reduce time-to-market** for new services, ensuring that more innovative solutions are accessible to government agencies sooner.

3. Develop **pre-authorized compliance packages** that allow smaller CSPs to **inherit security controls** from established, larger cloud service providers (such as AWS, Azure, or Google Cloud) that have already met federal compliance standards. These packages would include baseline security controls and shared responsibility documentation, enabling smaller CSPs to build on the security foundation of larger providers while focusing their compliance efforts on specific service-level requirements.

    a. The GSA Administrator should recommend that **FedRAMP PMO**, in collaboration with **large CSPs** and **third-party assessors (3PAOs)**, establish these pre-authorized packages with clear guidelines for inheritance of controls. The **FedRAMP Board** can oversee the implementation to ensure consistency and security.

    b. By leveraging the **control inheritance model**, smaller CSPs can **reduce the scope and cost of their compliance assessments**, focusing only on areas unique to their services. This would **accelerate the authorization process**, encourage innovation, and increase the availability of secure cloud solutions in the federal marketplace. Additionally, it would **reduce redundant compliance efforts** and foster closer collaboration between larger and smaller CSPs in delivering secure cloud services to government agencies.

Committee Notes:

- Continue the journey and emphasize the importance of Agencies to accept the FedRAMP PMO as the central authorizing authority for new entries into the FedRAMP marketplace to remove the search for sponsoring agencies process as a barrier. (Kayla)
- Work to reduce the documentation burden that comes with FedRAMP which includes hundreds of pages of explanations, filling out of multiple attachments, and requirements around various diagrams. (Kayla)

- MV: Barrier to entry = financial, technical, operational
- MV: Impact to innovation. What is the outcome of the current state? High cost and complexity should be emphasized.
- Bill: Identified Problem: Resources, specifically bottlenecks of 3PAOs not having enough staff to respond. Not having enough 3PAOs in the community.
    - Marci: Not a 3PAO bottleneck. Issue with time to get through the process for CSPs. Phantom requirements and things that don't come up until the very end. Some know about it, some don't do to frequency of use. Increasing transparency in the FR program is key. Increasing speed of publishing this information is also key. Allowing CSPs to realize the FR benefits faster.
        - CSP education issue of being ready v wanting to start immediately.
- JK: Agency sponsor is the only way to get authorized right now. Agencies don't have resources to review packages at the level needed. How can we simplify the ATO work for the agency?
    - JK: Often times, CSPs entering the FedRAMP journey face huge upfront costs whether it be hiring consultants to manage the arduous amounts of paperwork, building a new Gov't only environment, retrofitting existing environments, paying a 3PAO for the assessment etc. often with no initial investment from agencies. Agency Sponsorship is difficult to achieve and is one of the hardest parts of receiving authorization and is the current only path to getting authorized.
    - Daniel: Agency sponsorship program for education. Education of putting the work up front will go a long way, but need an incentive to 1) sponsor and 2) work with other agencies. Have experienced agencies work with less experienced ones to get through the process.
    - Marci: Current PMO "queue" is 30 weeks and that starts after an agency ATO is granted
- Branko: **Little info on actual barriers to entry. Issue w/ agency sponsorship is clear. No details on costs of resources and time. Why does it take 18mo to ATO? What does that look like? Need to better understand the timelines and costs. Where are those costs and how can we recommend improvements?**
    - How do we know these rec's are prioritized and hitting the most important barriers to entry?

Priority 2: Identify and publicly document ways to expedite the authorization process for CSOs – explore agile authorizations and other potential cost reductions, both labor and financial, with a focus on small businesses, e.g. ensure minimum risk threshold / minimum acceptability standardized baselines for sponsoring agencies and 3PAOs.

PROBLEM STATEMENT: The current authorization process for Cloud Service Offerings (CSOs) is overly complex, time-consuming, and costly, particularly for small businesses. Inconsistent validation of requirements and high compliance costs limit participation from smaller Cloud Service Providers (CSPs), reducing competition and slowing cloud adoption by federal agencies. A more efficient, standardized process is needed to lower barriers to entry, foster innovation, and ensure timely deployment of secure cloud solutions.

ACTIONABLE, SPECIFIC RECOMMENDATIONS (with projected benefits):

1. Explore the possibility of splitting out the authorization process into smaller approval stages that allow CSPs to begin selling as an "authorized" CSP. Even if there are variations to what they are allowed to sell or promote based on their stage. This would help reduce the time to value for CSPs during the initial authorization phase.

2. For continuous authorizations/monitoring, create an inheritance standard for common upgrades like OS to avoid the need for everyone to do a SCR. This would reduce the overhead for security teams and the amount of time for the back and forward.

3. Explore a program or exception process for CSPs that expands the permissible use of non-FedRAMP authorized vendors, thereby reducing the cost burden against those vendors who charge more and require additional configurations in order to use their FedRAMP offering (vs. their commercial offerings).

4. Task OMB (or FedRAMP Board or FedRAMP PMO) to develop and issue clear and authoritative guidance on thresholds for types of cloud offerings that DO NOT require (FedRAMP) ATO. This is a low hanging fruit and a barrier to entry that would significantly reduce the burden on both agencies and small CSPs for using small scale cloud offerings that do not require lengthy and expensive ATO process.

5. Develop **agile authorization pathways** that prioritize **critical security controls** early in the **Authority to Operate (ATO)** process. This approach would allow Cloud Service Providers (CSPs) to demonstrate compliance with the most **high-impact security controls** first (such as access control, encryption, and incident response). Once these essential controls are validated, CSPs could receive provisional ATOs for lower-risk services or environments, while continuing to meet remaining requirements for full authorization.

    a. The GSA Administrator should recommend that **FedRAMP PMO**, in collaboration with **sponsoring agencies** and **3PAOs**, design these pathways to prioritize critical controls, ensuring agencies can issue **provisional ATOs** more quickly for services that meet baseline security requirements.

    b. By focusing on **critical controls** at the start, CSPs can achieve **early provisional authorizations** for lower-risk services, reducing time-to-market while maintaining strong security. This would allow agencies to benefit from faster cloud adoption while ensuring that the most critical security risks are addressed upfront, creating a more efficient and secure cloud authorization process.

6. Establish **minimum standardized baselines** for security controls based on risk thresholds, uniformly accepted by agencies, 3PAOs, and CSPs. These baselines should focus on key security requirements, reducing redundancies and complexity by creating a clear set of expectations for all parties involved.

    a. The GSA Administrator should recommend that **FedRAMP PMO**, **CISA**, **NIST**, the **Office of the Federal CIO at OMB**, and sponsoring agencies collaborate to create and publicly document these **risk-based baselines**. CISA will contribute its cybersecurity risk expertise,

and the Office of the Federal CIO will ensure alignment with broader federal IT modernization and security policies.

b. Standardized baselines would reduce the burden on CSPs by providing **consistent, clear expectations** across agencies, while ensuring that security risks are appropriately managed. This would streamline the compliance process, accelerate authorizations, and encourage more CSP participation in the federal market. The inclusion of the **Office of the Federal CIO** ensures these efforts are coordinated with government-wide IT security and modernization strategies.

c. Recommend that GSA Administrator task the FedRAMP PMO to work with CISA, NIST, and other federal and industry partners to prioritize cybersecurity controls (by applying threat modeling or similar methodology) and determine Top X list of most critical controls. A smaller subset of prioritized controls (for both implementation and assessments) would allow for faster authorization process and reduction of overall cost to achieve an ATO.

7. Explore and establish **financial support or incentive programs** (e.g., grants or cost-sharing models) to help small businesses cover the initial labor and financial costs associated with compliance. This could also involve subsidies for assessments or leveraging public-private partnerships to lower entry barriers.

    a. Recommend **GSA's Office of Small Business Utilization, the Small Business Administration (via appropriations), and OMB** explore these incentives, with funding mechanisms supported by **Congress** or public-private partnerships.

    b. Offering financial incentives and cost-sharing opportunities will **increase participation from small businesses**, resulting in a more competitive and innovative cloud market. This will also lower the financial burden of achieving compliance for smaller players.

Committee Notes:

- (Kayla) One note on this goal - We didn't add in a lot of clarity around which authorization process we are discussing here, so I decided to take the approach of introducing recommendations for initial authorizations and continuous engagements like SCRs and Continuous Monitoring:
    - Explore the possibility of splitting out the authorization process into smaller approval stages that allow CSPs to begin selling as an "authorized" CSP. Even if there are variations to what they are allowed to sell or promote based on their stage. This would help reduce the time to value for CSPs during the initial authorization phase.
    - For continuous authorizations/monitoring - Create an inheritance standard for common upgrades like OS to avoid the need for everyone to do a SCR. This would reduce the overhead for security teams and the amount of time for the back and forward.
    - Explore a program or exception process for CSPs that expands the permissible use of non-FedRAMP authorized vendors, thereby reducing the cost burden against those vendors who charge more and require additional configurations in order to use their FedRAMP offering (vs. their commercial offerings).

        - Note on thoughts/intent * One of the secondary effects of being FedRAMP authorized is that any vendors in your supply chain must also be FedRAMP authorized. This creates a small circle of premium offerings that are all charging premium costs and increases the cost of doing business for the whole ecosystem. I will note that this is addressing a symptom of the high expense of FedRAMP for CSPs and not the root cause of the program being expensive to maintain authorization under.
- Branko: Come up with guidance on the thresholds/exceptions for ATO authorization.
    - Michael: Clear definition of CUI from the government would be helpful.
- Larry: What are absolute "musts," clear pass/fail, and what about the others? What is the next tier of requirements that are aggregated? Some percent of these must be met to meet the threshold. Red and yellow controls could be a best practice.
-
-

Priority 3: Identify best practices and recommendations on how FedRAMP can make progress with commercial reciprocity using different security frameworks

PROBLEM STATEMENT:

ACTIONABLE, SPECIFIC RECOMMENDATIONS (with projected benefits):

1. xxx
2. xxx
3. xxx

Priority 4: Identify what is needed to support OSCAL adoption and if there are any barriers to OSCAL interoperability within the CSP and agency GRC ecosystem that need to be addressed

PROBLEM STATEMENT:

ACTIONABLE, SPECIFIC RECOMMENDATIONS (with projected benefits):

1. xxx
2. xxx
3. xxx

[Committee Staff will work with Chair to complete the conclusion/summary of benefits after the recommendations are completed]