February 17, 2025
Federal Risk and Authorization Management Program
General Services Administration
1800 F Street, NW Suite 400
Washington DC, 20405

Submitted electronically via public comment spreadsheet.

Re: RFC004 FedRAMP Boundary Policy

The Cloud Service Providers-Advisory Board (CSP-AB) appreciates the opportunity to comment on the proposed changes outlined in RFC-0004.

The Cloud Service Providers - Advisory Board (CSP-AB) represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

By way of introductory remarks, the Cloud Security Provider Advisory Board (CSP-AB) recognizes that the Federal Risk and Authorization Management Program (FedRAMP) provides a standardized security assessment and authorization approach that saves the federal government significant resources by eliminating redundant agency security assessments. This "do once, use many" framework enables cloud service providers (CSPs) to undergo a single comprehensive security evaluation that can be leveraged across multiple federal agencies, reducing time-to-market while ensuring consistent and rigorous security standards for federal cloud deployments.

According to the U.S. Government Accountability Office (GAO) in its 2024 Report to Congressional Committees on Cloud Security, federal agencies increased their use of FedRAMP-authorized solutions by 60% between 2019 and 2023. This rapid growth underscores FedRAMP's critical role in enabling faster, more secure, and cost-effective cloud adoption across government agencies. As cloud technology continues to evolve, FedRAMP's continuous monitoring framework must adapt to ensure that security requirements remain effective and scalable while maintaining its efficiency benefits.

As an advocate for robust and scalable cloud security frameworks, we applaud FedRAMP's commitment to enhancing continuous monitoring processes, streamlining security control assessments, and fostering greater efficiency in risk management. These updates will significantly improve the ability of Cloud Service Providers (CSPs) and federal agencies to maintain compliance while addressing emerging cybersecurity threats in an evolving digital landscape.

We appreciate FedRAMP’s ongoing efforts to refine these standards and thank you for considering our recommendations. We look forward to continued collaboration to ensure the highest levels of security, efficiency, and innovation in federal cloud adoption.

Editorial comments

> *This policy explicitly limits the FedRAMP boundary to a subset of the full traditional authorization boundary. If a SaaS offering runs on a FedRAMP authorized PaaS then both the SaaS offering and the aspects of the PaaS used by the SaaS offering would be inside the agency Authorization to Operate boundary but the FedRAMP authorization will only include the SaaS offering and its configuration of the PaaS. This is difficult to convey effectively in general due to the many dimensions of reuse. Examples are recommended, but how can this be standardized clearly without examples?*

It may be beneficial to explicitly state that if a Cloud Service Offering (CSO) leverages authorizations from other Cloud Service Providers (CSPs), the customer responsibilities outlined in the responsibility matrix fall under the CSO’s obligations as a customer of the upstream CSP. These responsibilities must be documented and validated during assessments.

> *This draft introduces the plain language idea of “handling” federal information as inherently inclusive of everything one can do with information without continuously providing a long list of verbs (“create, collect, process, store, transmit, access, maintain, use, disseminate, disclose, dispose, etc.”). Is this sufficiently clear?*

The existing language appears sufficiently clear, particularly if similar clarifications are provided in the introductory sections of related documents.

> *FRR211: This rule is intended to convey that restrictions on external connections may not be used by a cloud service provider to deny access to the owner of federal information in a cloud service offering. A cloud service offering may allow agency authorized services to interconnect with the cloud service offering and only needs to document the relevant mechanisms within the cloud service offering. For example, if a cloud service offering allows authenticated API access to information, then any system used by the agency to access that information is outside the FedRAMP boundary but not prevented under this rule. This is a difficult process rule to communicate. Providing comment on improving clarity here would be appreciated.*

To improve clarity, it should be stated that any external systems procured by a CSP/CSO for use with federal information must receive approval. Additionally, if agencies independently procure services and use them to access the CSO through existing channels—such as readily available APIs with established rate limits—the CSO is not permitted to restrict such access.

Policy comments

Section 1: Policy Overview

“The FedRAMP boundary includes all aspects of the CSO, including external services, that...directly impact the confidentiality, integrity, or availability of federal information”.

We believe this language is ambiguous and requires more specificity. We therefore suggest the following amendment:

> “The FedRAMP boundary includes all aspects of the CSO, including external services, that...have privileged access to federal information such as security tools that ensures confidentiality, integrity and availability of federal data and metadata”.

We believe this provides clearer guidance for components to determine applicability

FRR202

“CSPs shall include any components required to be installed or run on a tenant system in order to use the CSO and may include additional optional components if they are included in the SSP.”

We appreciate FedRAMP's intent to ensure transparency regarding components deployed on tenant systems. However, the current wording may lead to ambiguity regarding the CSP’s responsibility versus the customer’s responsibility for such components. Some components required for the CSO’s functionality—such as agents, client-side applications, or integrations—may be customer-managed, making their inclusion within the CSP’s authorization boundary problematic.

Furthermore, while these components should be considered in security assessments, treating them as fully within the CSP's boundary could create confusion regarding operational ownership and liability.

We suggest refining the language to ensure that security and assessment expectations are met while maintaining a clear separation of responsibilities:

> "CSPs shall document any components required on a tenant system to use the CSO. A 3PAO shall assess, penetration test, and validate responsibility scope of these components. The validation must ensure that customer-designated responsibilities—such as network security, endpoint protection, user access, and patching—are both feasible for the customer and explicitly out of scope."

This revision ensures that:

- Security testing covers all relevant components, including those running on tenant systems.
- Best-practice security is assessed as part of the overall solution.
- Customer responsibilities remain explicitly separate, avoiding unnecessary CSP liability for customer-managed aspects.

This clarification would improve security expectations while ensuring that CSPs and customers maintain appropriate and clearly defined responsibilities.

FRR208

This subsection of the *FedRAMP Boundary Definition* section reinforces the previously stated requirements, stating: *"CSPs shall ensure that security and administrative configuration, secrets, key material, and agents are managed within the FedRAMP boundary and are documented within the SSP."*

This requirement introduces potential scalability and cost challenges for Authorizing Officials (AOs) managing hundreds or thousands of agents. Additionally, it raises concerns about how CSPs will deploy, upgrade, and maintain agents on agency endpoints.

FRR209

"CSPs shall document and maintain information exchange agreements for all external systems within the FedRAMP boundary. This shall include the information types, encryption employed, ports/protocols/services used, access levels, and the requirement to meet FedRAMP security requirements."

It is the belief of the CSP-AB that an information exchange agreement was needed with a system that is outside the boundary, meaning we find the language "within the FedRAMP boundary" confusing.

We therefore recommend re-defining with exclusions and example of what is in scope:

> Maintain information exchange agreements where persistent bi-directional data flow occurs between the FedRAMP authorized boundary and other information systems.
>
> Exclusions:
>
> - Connections between components within the same FedRAMP boundary
> - Temporary/one-time data exchanges
> - Public-facing web services
> - Read-only data feeds
> - Standard internet access
> - Ad-hoc or user-initiated transfers

Example of what would be in scope:

- Regular automated data synchronization between boundaries

Example of what would be out of scope:

- One-time data migration
- User downloads/uploads
- Occasional system maintenance connections

We appreciate FedRAMP’s continued engagement on these topics and would be delighted to discuss any of these recommendations in greater detail.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

lnavaratnam@csp-ab.com

http://csp-ab.com