Published on *The National Law Review* https://natlawreview.com

FedRAMP Releases New Draft Authorization Boundary Guidance

Article By:

Townsend L. Bourne

Daniel J. Alvarado

Over the last few years, the Federal Risk and Authorization Management Program (“FedRAMP”) Program Management Office (“PMO”) has released two draft guidance documents related to defining the applicable boundary for security assessments of cloud service offerings, but final versions were never released. On January 16, 2025, FedRAMP released another draft authorization boundary guidance document (RFC-0004). FedRAMP’s authorization boundary guidance is “the most frequently requested policy update” as it forms the foundation for determining the scope of review for assessment and authorization. The new draft currently is open for public comment through February 17, 2025.

Refresher

An authorization boundary is defined in the National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-37, *Risk Management Framework for Information Systems and Organizations*, as “all components of an information system to be authorized for operation by an Authorizing Official and excludes separately authorized systems to which the information system is connected.”

We have been following the FedRAMP authorization boundary guidance for a few years (see our blog here). During this time, the FedRAMP PMO has published the current authorization boundary guidance and two draft versions (Version 2.0 and Version 3.0). In these draft guidance documents, FedRAMP guidance focused on two types of information: (1) Federal data and (2) Federal metadata. Federal metadata was later broken out into several different types of data such as Direct-impact, Indirect-impact, Low and Limited-impact data, and Corporate data. The new draft guidance document largely moves away from use of these data subcategories and instead focuses on providing streamlined requirements for defining the authorization boundary.

New Draft FedRAMP Authorization Boundary Guidance

The new draft authorization boundary guidance seeks to clarify and streamline which systems and data fall within the FedRAMP boundary. The FedRAMP boundary should include all services that:

1. Handle federal information; and/or
2. Directly impact the confidentiality, integrity, or availability of federal information.

The new guidance provides the following example of services that are included within the authorization boundary:

This includes all services to be consumed by tenants/customers and the underlying components, infrastructure, and services (including external services), that handle federal information as part of the CSO and the related organizational users operating the service. It also includes privileged security tooling, authentication systems, management/orchestration, and keying material and secrets.

Services not meeting these criteria should be excluded from the authorization boundary, with appropriate justification and risk-based review. Ancillary services posing negligible risk to federal information are explicitly outside the scope. The draft FedRAMP authorization boundary guidance provides the following description of ancillary services that may be outside of the FedRAMP boundary:

Examples of ancillary services that may be outside the FedRAMP boundary include corporate email services, development environments, and customer service systems where a loss of confidentiality, integrity, or availability is not likely to directly affect federal information within the CSO.

One area of focus in the draft FedRAMP authorization boundary guidance is limiting the assessment to services whose compromise could pose significant risks to federal information security (i.e., services that are not FedRAMP authorized). In order to do so, the guidance encourages the reuse of FedRAMP authorized external services to minimize duplication of effort. In other words, the guidance encourages the use of other FedRAMP authorized cloud services to reduce the need for additional assessment of the particular external service. This will allow focus on assessing customer configurations rather than the entire external service.

Requirements for CSPs

The new draft authorization boundary guidance provides requirements for CSPs regarding boundary definition, protection of information, and restrictions on inbound and outbound connections. Below are a few key requirements in the draft:

- CSPs must define the FedRAMP boundary to include all relevant services and components that handle federal information and/or directly impact the confidentiality, integrity, or availability of federal information.
- CSPs must document components, data flows, encryption, and access points in the System Security Plan.
- CSPs must ensure federal information is not reused for shared purposes without customer approval and document information exchange agreements.
- CSPs must continuously update boundary documentation as the system architecture evolves and as protections or data flows change. These updates must be made promptly in the SSP, as well as in continuous monitoring reports and Plan of Action and Milestones ("POA&Ms").
- CSPs shall not permit any systems outside the FedRAMP boundary to directly access federal information or make changes to the security of the FedRAMP boundary without approval by the owners of the federal information.
- CSPs must document all connections established between the FedRAMP boundary and systems in the environment of operations, including the data types, encryption employed,

ports/protocols/services used, the level of access, and the service or component involved.

Companies currently preparing for the FedRAMP authorization process should continue utilizing the current final authorization boundary guidance available on the FedRAMP website. This draft authorization boundary guidance can be used as a reference to inform your analysis to define your authorization boundary.

Role of Independent Assessors

Independent assessors (e.g., third party assessment organizations (“3PAOs”)) are responsible for testing all components within the authorization boundary and evaluating connections to external systems. The Independent Assessor also must validate data flows and ensure they do not pose direct security risks or provide privileged access to federal information.

Conclusion

The new draft FedRAMP authorization boundary guidance aims to enhance the efficiency of the authorization process by clearly defining the scope of assessment and focusing resources on high-risk areas. Feedback from industry will be critical for developing the final guidance that has been years in the making to ensure it meets the needs of all stakeholders while maintaining robust security standards. FedRAMP anticipates multiple rounds of comments for “the most frequently requested policy update” to ensure the appropriate guidance is provided in the final version.

The comment period currently is open until February 17, 2025. Comments can be submitted through various channels, including a discussion forum through GitHub, a public comment spreadsheet available on the draft guidance webpage, and email to pete@fedramp.gov with subject “RFC 0004 Feedback.”

National Law Review, Volume XV, Number 29

Source URL:https://natlawreview.com/article/fedramp-releases-new-draft-authorization-boundary-guidance