SheppardMullin
Government Contracts & Investigations Blog
Latest updates on Developments Affecting Government Contracts & Investigations

Watch Your Boundaries – FedRAMP Releases Draft Authorization Boundary Guidance for Public Comment

By Townsend Bourne, Daniel Alvarado & Lillia Damalouji* on July 28, 2021

POSTED IN CYBERSECURITY, INFORMATION TECHNOLOGY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The FedRAMP Program Management Office is seeking comments on its draft **FedRAMP Authorization Boundary Guidance, Version 2.0**, released on July 13, 2021. The public comment period currently is open and closes on September 13, 2021.

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." Put simply, an authorization boundary is the "foundation on which the rest of a system security plan is built."**[1]**

The FedRAMP Authorization Boundary Guidance (the "Guidance") provides Cloud Service Providers that are pursuing or holding a FedRAMP Authorization with guidance for developing and maintaining an authorization boundary. Cloud Service Providers must clearly define the authorization boundary for their Cloud Service Offering to help the government understand what is being secured, tested, and authorized when issuing a FedRAMP Authorization.

The Guidance initially was issued to assist Cloud Service Providers in identifying their Cloud Service Offering authorization boundary to support their FedRAMP authorization package. Version 2.0 is designed to provide additional detail on how to describe and illustrate the Cloud Service Offering's authorization boundary, data flow diagrams, and network interconnections.

The proposed Version 2.0 Guidance provides an overview of key definitions and requirements outlined in NIST SP 800-37, NIST SP 800-53, ***Security and Privacy Controls for Information Systems and Organizations***, and Office of Management and Budget Circular A-130, as well as an overview of the following concepts:

- **Defining Your Authorization Boundary in the Cloud**: Cloud Service Providers must describe types of data, flow of data, treatment of federal data and federal metadata, and external systems processing, transmitting, or storing federal data and federal metadata on behalf of the Cloud Service Provider's system.
- **Federal Data in the Cloud**: Cloud Service Providers must account for, and include within their authorization boundary, all federal data including metadata as defined in NIST SP 800-60, ***Guide for Mapping Types of Information and Information Systems to Security Categories***.
- **Federal Metadata in the Cloud**: Cloud Service Providers must account for (1) federal metadata and (2) corporate metadata, each having their own security considerations and requirements.
- **Interconnections in the Cloud**: Must be reviewed by an agency Authorizing Official to ensure all federal data and metadata residing within or leaving the Cloud Service Provider's system is adequately protected.
- **External Services in the Cloud**: While Cloud Service Providers are permitted to augment or support their systems through the use of external services, Cloud Service

Providers must clearly document and describe these external services in their authorization boundary.

- **Leveraging External Services with a FedRAMP Authorization**: The Guidance describes how a Cloud Service Offering may leverage an underlying service from a FedRAMP Authorized Cloud Service Provider.
- **Corporate Services**: These corporate services exist outside of the authorization boundary and must not contain any federal data or unauthorized metadata unless the Cloud Service Provider owns and operates the system and attests that the corporate system meets the security requirements outlined in NIST SP 800-171, ***Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations***, or be in a Cloud Service Offering at the same security level.

The Guidance also includes data requirements, agency-specific security requirements, and an appendix focused on developing authorization boundary, network, and data flow diagrams.

Note that Section 3 of the Biden Administration's May 2021 **Executive Order on Improving the Nation's Cybersecurity** (No. 14028), which we have previously covered (**here**), directs the Federal Government to "take decisive steps to modernize its approach to cybersecurity" to include "modernizing FedRAMP," and "accelerate movement to secure cloud services." Although the Guidance does not expressly reference the May 2021 Executive Order, the Guidance aims to further clarify the existing Authorization Boundary Guidance to enable Cloud Service Providers to more quickly and securely obtain FedRAMP Authorization, which fits squarely within the Executive Order's purpose.

With the comment period for this Guidance concluding on September 12, 2021, it is important for Cloud Service Providers pursuing or maintaining a FedRAMP Authorization to provide industry perspective as FedRAMP seeks to provide detail and clarify existing guidance. Further, Cloud Service Providers should familiarize themselves with the evolving requirements for cloud computing technology and federal information security relevant to FedRAMP. More information on the commenting process can be found on the **GSA website**.

*Lillia Damalouji is a Summer Associate in the firm's Washington, D.C. office.

FOOTNOTES

[1] FedRAMP Authorization Boundary Guidance, Version 2.0, at 10.

Government Contracts & Investigations Blog

Copyright © 2022, Sheppard, Mullin, Richter & Hampton LLP. All Rights Reserved.