CYSE 425W Policy Analysis Paper

Securing the Cloud, Shaping the Policy: The Politics surrounding FedRAMP

Gabrielle Gaston

In an industry where cloud computing encompasses all sectors from high level national defense systems to standard organizational administrative tasks, the discussion of how the federal government secures its digital infrastructure has become controversially political. At the heart of this debate stands the Federal Risk and Authorization Management Program (FedRAMP), a framework originally designed to streamline secure cloud adoption by reducing redundant security reviews. Over time, however, FedRAMP has grown beyond a technical compliance tool, gaining traction as a politically backed program that reflects the evolving interests of national security, federal procurement, administrative capacity, and private industry. The political implications of FedRAMP are evident in the ways elected officials and senior ofiicials have responded to the program, the motivations behind those responses, and the broader ripple effects for federal governance and the rapidly expanding cloud services marketplace (Federal Risk and Authorization Management Program, n.d.; Government Accountability Office, 2024).

FedRAMP's institutionalization, originating within the General Services Administration (GSA) and coordinated across agencies, has political relevance stemming from centralized authority over cloud security policies that were previously delegated across agencies. Centralization yields predictable standards and economies of scale for authorization, but it also concentrates discretionary power in a small set of actors. This disproportionate hierarchy created a lot of controversy surrounding FEDRamp. As a result, policymakers had to balance supporting a trustworthy, uniform system that protects sensitive federal data, improves efficiency to remove obstacles that slows agency modernization or is perceived as giving the bureaucracy excessive gatekeeping power. The program's governance and reform debates, including the 2025 "FedRAMP 20x" modernization effort, reflect the adjustment of political judgments about which objective should dominate (Federal News Network, 2025; GSA, 2025).

Consequently, policymaker's decisions on FedRAMP reveal underlying political trade offs. On one hand, congressional oversight bodies and the Government Accountability Office have emphasized stringent security controls driven by concerns about national security, privacy, and the integrity of federal systems. On the other hand, agencies, industry groups, and some executive branch reform advocates have criticized FedRAMP as slow and costly, arguing it hinders access to commercial innovation and increases procurement costs. These competing pressures explain policy shifts such as the 2024 through 2025 modernization that attempt to speed authorizations without weakening baseline protections ultimately avoiding "an explicitly political compromise to reconcile security and competitiveness" (Government Accountability Office, 2024; McLaughlin, 2020; Office of Management and Budget, 2024).

This further supports to the stance that different political actors analyze FedRAMP through lenses shaped by political party affiliation, opinions of elected officials, and institutional missions. Therefore, Congress tends to treat cyber and cloud security as oversight and accountability issues while lawmakers from districts with large federal contractors or tech employers push for faster, less oppressive processes to support local economies. Presidential administrations reinforce digital modernization as an executive priority, yet each sector's administration framing varies. Despite the fact thst some insist rapid adoption to streamline the process of modernizing services, others prioritize strengthening controls in the face of geopolitical cyber threats before initiating the adoption. These political incentives help explain inconsistent reform waves such as the FedRAMP 20x initiative and differing statements from the GSA, OMB, and agency CIO councils calling for both speed and robust assurance (GSA, 2025; McGillivray, 2016).

Analyzed through a timeline perspective , the political decisions around FedRAMP have cascading consequences. By establishing a common authorization pathway, FedRAMP creates significant market advantages for vendors who can afford compliance costs. Raising entry barriers and shaping vendor politics creates standards where larger cloud firms often gain superior access to federal contracts. Secondly, modifications to the program redisperse political benefits and influence assorted industry actors and agency buyers. Third, from a public policy perspective, FedRAMP demonstrates policy feedback dynamics where the program's existence changes future political incentives. Scholars of policy drift and institutional change argue this feedback loops create complexity that sway long term outcomes for governance and public accountability (Galvin & Hacker, 2019; Birkland, 2021).

Recent policy instruments, including GAO evaluations, OMB memos, and the FedRAMP 20x overhaul, illustrate how policymakers respond to competing pressures. This is revealed through GAO reviews impelling FedRAMP to improve consistency and document savings. OMB and GSA memos articulate modernization goals that reflect political commitments to both cybersecurity and technological leadership, while organizations that prioritize AI cloud services reveal how sector specific political pressures reform program priorities. In a combined effort, these responses shape who benefits from the program, how quickly agencies transition, and how transparent the authorization process becomes (Government Accountability Office, 2024; Office of Management and Budget, 2024).

In conclusion, FedRAMP is not merely a technical compliance framework. With the correct enforcement, it is a political instrument that embodies risk, procurement, industrial policy, and bureaucratic authority. The program's ongoing reforms and controversies illustrate how cyber policy is intertwined in political incentives and institutional constraints. For policymakers, the solution is that designing cyber governance mechanisms requires explicit attention to distributional effects, transparency, and mechanisms to manage policy feedback. Without these considerations, the program's technical goals are at risk of being crippled by political tension and unintentional market heirarchy.

References

Birkland, T. A. (2021). Governing in a polarized era: Federalism and emergency management. Frontiers in Political Science. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8385820/

Federal News Network. (2025, August 5). FedRAMP 20x pilot finds initial success with four approvals. https://federalnewsnetwork.com

Federal Risk and Authorization Management Program. (n.d.). FedRAMP. https://www.fedramp.gov

Galvin, D., & Hacker, J. (2019). The political effects of policy drift: Policy stalemate and American political development. Institute for Policy Research Working Paper. Northwestern University.

General Services Administration. (2025, August 11). GSA celebrates major milestones in FedRAMP cloud modernization. https://www.gsa.gov

Government Accountability Office. (2024, January 18). Cloud security: Additional actions needed to strengthen federal use of cloud services (GAO-24-106591). https://www.gao.gov/assets/gao-24-106591.pdf

McGillivray, K. (2016). FedRAMP, contracts, and the U.S. federal government's move to cloud computing. Stanford Technology Law Review.

McLaughlin, M. (2020). Reforming FedRAMP: A guide to improving procurement and risk management. Information Technology and Innovation Foundation. https://itif.org

Office of Management and Budget. (2024). M-24-15: Modernizing the Federal Risk and Authorization Management Program (FedRAMP). White House.