February 1, 2023

The Honorable Shalanda Young
Director, Office of Management and Budget

The Honorable Robin Carnahan
Administrator, General Services Administration

Re: Federal Risk and Authorization Management Program (FedRAMP)

Dear Director Young and Administrator Carnahan,

In 2011, when Federal Chief Information Officer (CIO) Steven VanRoekel signed the initial memo that created the Federal Risk and Authorization Management Program (FedRAMP),[1] he was overseeing a federal government comprising a mix of on-premise servers, local area networks, and some adventurous deployments of cloud technology that varied by agency. Cloud deployment was encouraged, where possible, but was not expected.

Over a decade ago, agency CIOs and their teams sometimes considered cloud services when investing their insufficient development, modernization, and enhancement (DM&E) dollars. The systems and data identified for migration to cloud instances were typically viewed as pilot projects and did not include what agencies now call "high-value assets."[2] While technologists and IT leaders at agencies considered cloud adoption as the path forward, the agency leaders, mission owners, budget executives, and others did not yet understand the opportunities and efficiencies provided by modern cloud-based solutions.

Twelve years later, much has changed. Almost all federal agencies are migrating high-value assets, systems, and services to cloud environments. Many have multiple cloud deployments that range from infrastructure to software applications. Agency leaders include requests in their budgets for modern, commercial cloud services and technologies that will underpin their mission delivery capabilities.

What hasn't changed, however, are the major policy parameters that govern how agencies manage risk associated with cloud adoption. Additionally, the FedRAMP program at the General Services Administration — including its Joint Authorization Board (JAB) and technical reviewer teams — has been woefully underfunded and has not grown at the pace of agency cloud adoption. Over the last twelve years, the

[1] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
[2] https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

FedRAMP leadership has partnered with agencies and industry to improve its processes: streamlining initial authorizations and promoting reuse of those authorizations. However, even as agencies' desire to adopt secure cloud services has grown exponentially, the policies that govern FedRAMP and a lack of adequate funding have continued to be limiting factors.

Fortunately, Congress, through the passage of the FedRAMP Authorization Act in FY 2023 National Defense Authorization Act (NDAA) and the Consolidated Appropriations Act of 2023 (FY23 Omnibus), provided the legislative direction and the additional funding to modernize the program to meet the current and future technology needs of a model digital government. The FedRAMP Authorization Act provides the Administration with a mandate to rethink how FedRAMP supports risk management across agencies while lowering the barriers to access the latest commercial solutions. The law requires the White House Office of Management and Budget (OMB) to issue guidance to departments and agencies that does the following:

1) Requires FedRAMP authorizations for "all necessary and appropriate cloud computing products and services";[3]
2) Describes the responsibilities of FedRAMP and the FedRAMP Board to accelerate cloud adoption across the federal government;
3) Establishes a process to review authorization to operate (ATO) packages to promote reuse;
4) Allows for oversight of the FedRAMP Board and Program Management Office (PMO); and
5) Promotes consistency of assessments and authorizations.

Additionally, the FedRAMP Authorization Act directs the Administration to rethink its approach to the Joint Authorization Board and requires public, on-the-record interactions with industry stakeholders.

Given these mandates, OMB, and the General Services Administration (GSA) should prioritize several actions as they update the FedRAMP authorization policy and additional FedRAMP guidance. Specifically, the Administration should:

1) **Encourage real risk management from the authorizing officials at agencies.** Agencies often default to higher levels of required security control baselines than may be needed for a particular system. Procurement officials and mission owners default to an increased number of controls because authorizing officials believe this protects them from oversight and other repercussions in the wake of a security incident. Additionally, agencies are not incentivized to tailor the security controls to the minimum acceptable risk in order to quickly bring a tool or service online. This approach can both limit government access to only those technologies that have achieved the highest baseline and delay the adoption of a technology until it meets the highest baseline controls. By encouraging tailored

[3] https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf

risk management,[4] agencies can more nimbly adopt technology at an appropriate security baseline while staying compliant with all Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) requirements and expediting the adoption of technology.

2) **Incentivize agencies to sponsor new cloud services and solutions.** Sponsoring a FedRAMP authorization for a Cloud Service Provider (CSP) can be a time-consuming and resource-intensive process for authorizing officials. One agency estimated that it can sponsor eight to ten FedRAMP authorizations a year by employing four to five dedicated technologists and security professionals to support the work.[5] Only well-funded agencies with modernization-focused security and technology teams can afford to dedicate those resources to the effort. Through a combination of funding, personnel support, and public recognition, OMB and GSA can incentivize agencies to sponsor FedRAMP authorization packages and increase the number of products and services that can be accessed by government agencies. Additional resources provided in the FY23 Omnibus and the American Rescue Plan Act for the Federal Citizen Services Fund should be used by GSA to go beyond growing the capacity of the current processes and to think big about how to help accredit more CSPs and increase innovation across the federal cloud marketplace.

3) **Require all new security compliance programs across the government to build in reciprocity with FedRAMP.** From the Cybersecurity Maturity Model Certification (CMMC) at the Department of Defense to the new Security Software Development Framework (SSDF) attestation, new security compliance programs continue to leverage the same set of security controls. Additionally, there are many commercially recognized standards and certifications that leverage similar, if not identical, security controls. As the Administration moves forward with the development of rules and policies that will drive these additional compliance regimes, it should ensure that all overlapping requirements are captured and recognized. This will reduce the administrative burden for the government and the compliance burden of the cloud companies, and allow agencies to more quickly comply with these new security policies. A good example is the GSA's own procurement team, which has outlined that FedRAMP accreditation is sufficient for SSDF compliance.[6]

4) **Drive governance, objectivity, and consistency across the technical review process.** For the last decade, technical reviews of authorization packages have varied wildly based on the individuals performing the reviews. When companies have identified inconsistencies or have disagreed with technical reviewers, the FedRAMP program management office has not had the ability to drive

[4] This tailored risk management approach was also championed by the 2019 Cloud Smart Strategy: https://cloud.cio.gov/strategy/#security

[5] This statistic comes from an interview with an authorizing official and FedRAMP coordinator at a Chief Financial Officer (CFO) Act agency.

[6] https://www.gsa.gov/cdnstatic/MV-23-02_0.pdf

consistency across the various agency reviewers. OMB and GSA should create a governance structure that builds in a nimble, objective appeals process and couple that with additional automation during technical reviews. GSA should then invest the additional FY23 Omnibus resources in growing the number of technical reviewers across the agencies leveraging the governance structure to ensure consistency.

5) **Create a Federal Secure Cloud Advisory Committee that pulls from a wide range of industry partners, including cloud security vendors.** The FedRAMP Authorization Act requires GSA to build a 15-person committee that includes at least five representatives from cloud companies, including two small businesses. While the majority of the required participants are government agencies, GSA should consider including more than just the minimum required number of industry participants. Additionally, GSA should ensure that there is a process to continually refresh the industry participants on the committee through rotating, overlapping membership. Finally, as part of the Committee's three or more annual meetings, GSA should ensure that additional industry voices can participate through submitted questions, an "industry input" section of each meeting, or other avenues. Given the commercial cloud sectors' level of interaction with the program, guaranteeing a wide range of industry inputs will serve to strengthen the feedback from the new advisory committee.

6) **Build transparency into the reporting process.** The FedRAMP Authorization Act requires additional reporting to Congress from the FedRAMP Program Management Office (PMO) as well as the Government Accountability Office (GAO). The Administration should take advantage of these reporting requirements to identify and publish the authorities to operate (ATOs) issued by each agency for various Cloud Service Providers (CSPs). This will allow agency authorizing officials to understand what products and services are being leveraged by near-peer agencies. It will also allow commercial cloud solutions to build better integrations across platforms and services, giving agencies a broader selection of better-integrated cloud services and technologies, while saving resources.

7) **Don't forget about the little guys.** Small businesses drive innovation in almost every sector of the economy, including in cloud services. Agencies must still meet the targets for acquisitions of small business products and services. Given these requirements, the Administration should consider specific actions that will lower the barrier to entry into the federal marketplace for small, innovative cloud businesses. These actions could consist of providing grants to small businesses to pay for third-party assessments or creating additional "lanes" for approval and reuse of small business authorizations. The Administration should be creative in encouraging small businesses to participate in the FedRAMP marketplace to provide agencies with the best possible technologies to meet their dynamic missions.

8) **Provide multiple pathways for product improvements, modifications, and additions.** The current change control process disincentivizes continuous improvement due to a number of factors, including the rigid definitions of boundaries. There are some cloud companies that have created platforms and solutions focused on vertical integration. By considering solutions that have several components as modifications with inherited controls as opposed to new products, FedRAMP can grow its marketplace while potentially reducing the cost of compliance for companies interested in working with the federal government.

9) **Open the marketplace to include solutions that are in the process of becoming "eligible" for a FedRAMP authorization.** By allowing companies that are making investments in the necessary controls to participate in a marketplace, federal agencies will have a wider selection of services to consider. This can lower the barrier of entry into the federal marketplace as well, allowing non-traditional technology to test out the marketplace before investing significantly in the FedRAMP process. Additionally, GSA should consider capturing and publishing commonly accepted commercial certifications for those products that would like to participate in the FedRAMP marketplace but have not received a FedRAMP ATO. GSA should also consider aggregating FedRAMP "eligible" and FedRAMP "ready" companies into a centralized sponsorship directory that mission and enterprise owners can leverage when considering what products and services they would like to sponsor.

10) **Hold government off the shelf technology (GOTS) to the same standard as commercial off the shelf technology (COTS).** Given the legal requirement for commercial preference for products and services,[7] OMB and GSA should update authorization and risk management policies to drive consistency in their requirements and reviews of GOTS and COTS solutions. GOTS products should undergo the same compliance reviews, oversight, and security considerations as commercial products. If a waiver process is warranted for GOTS products, the bar for issuance of a waiver should be very high, and any GOTS solution waiver should be documented and reciprocally waived for similar commercial solutions.

11) **Appoint a FedRAMP coordinator at each agency and resource it effectively.** One of the biggest challenges for many technology companies attempting to partner with federal agencies is identifying an agency that wants to invest agency time and resources navigating the FedRAMP ATO process. To help with this challenge, the Administration should consider designating a FedRAMP coordinator focused on assisting agency mission and enterprise owners who want to onboard a new cloud product or service. Additionally, the Administration should work with agencies to build in budget requests for teams that can support the coordinator at each agency.

[7] https://www.govinfo.gov/content/pkg/USCODE-2021-title41/pdf/USCODE-2021-title41-subtitleI-divsnC-chap33-sec3307.pdf

To make the changes outlined above, the FedRAMP PMO will require additional sustained resources from its 2022 baseline budget. Fortunately, the Consolidated Appropriations Act of 2023 (FY23 Omnibus) provided GSA with a significant $35 million funding increase in the Federal Citizen Services Fund (FCSF). Additionally, the FY23 Omnibus included language allowing agencies to transfer unused, end-of-year funding into the FCSF for government-wide programs like FedRAMP.[8] The FedRAMP PMO should leverage these additional resources to invest in technical personnel, tools that can provide automation and continuous monitoring, wider adoption of Open Security Controls Assessment Language (OSCAL), and teams that can assist agencies in authorizing new cloud products and services. The funding can also directly support implementation of the actions outlined above while supporting agencies that have traditionally relied on other, better-resourced agencies to authorize new cloud products and services.

The speed of technological innovation is not slowing down. Agency leadership and mission owners will continue to demand access to the latest technology to meet the needs of the American people. Therefore, FedRAMP must evolve to become a risk management and authorization program that supports the expanding and dynamic technology needs of our digital government. The recent authorizing legislation provides the framework to reimagine FedRAMP in a way that keeps up with constantly accelerating demand and flexes to meet agency needs. The public and private sectors need to work closely together to develop a policy that encourages agencies to make risk-based decisions based on security threats and not perceived oversight. This is an opportunity for the Administration to develop a policy that allows FedRAMP to grow and change with the needs of government at the speed of technological innovation.

Sincerely,

The Alliance for Digital Innovation

CC: Mr. Jason Miller, Deputy Director for Management, OMB
Ms. Clare Martorana, Federal Chief Information Officer, OMB
Ms. Ann Lewis, Director Technology Transformation Service, GSA
Mr. Brian Conrad, Director FedRAMP PMO, GSA

[8] https://fcw.com/digital-government/2023/01/new-funding-flexibility-could-help-extend-reach-federal-citizen-services-fund/381515/