THE COALITION
FOR GOVERNMENT PROCUREMENT

December 22, 2023

Ms. Shalanda D. Young
Office of Management and Budget
Washington, D.C.

Subject: Comments on Draft Memorandum on Modernizing the Federal Risk Authorization Management Program (FedRAMP)

Ms. Young,

The Coalition for Government Procurement ("the Coalition") appreciates the opportunity to comment on the Office of Management and Budget's (OMB) October 27, 2023, Draft Memorandum on Modernizing the Federal Risk Authorization Management Program (FedRAMP). The purpose of the Memorandum is to implement the FedRAMP Authorization Act and provide an updated vision, scope, and governance structure for the FedRAMP program that is responsive to developments in Federal cybersecurity and substantial changes to the commercial cloud marketplace that have occurred since the program was established. The Coalition timely submits these comments within the comment period ending December 22, 2023.

By way of background, the Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through General Services Administration (GSA) contracts, including the Multiple Award Schedule (MAS) program. Coalition members also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for more than 40 years promoting the mutual goal of common-sense acquisition.

The Coalition supports the vision of the Draft Memorandum, which is to:

- Lead an information security program grounded in technical expertise and risk management;
- Rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures;
- Streamline processes through automation; and
- Leverage shared infrastructure between the Federal Government and private sector.

Each of these topics are addressed herein, along with suggested considerations.

Leverage shared infrastructure between the Federal Government and private sector.

The stated goal of FedRAMP was to accelerate safely the adoption of cloud products and services by Federal agencies, and to help those agencies avoid duplicating effort by offering a consistent and reusable security authorization process. To date, FedRAMP has not accelerated the adoption of cloud products and services by Federal agencies or reduced the duplication of effort at the pace desired. The Federal government lags behind other large enterprises in the adoption of cloud. Moreover, the process is not keeping pace with innovation in the cloud sector. A growing gap has opened between Cloud Service Providers' (CSPs) commercial and government offerings due to FedRAMP regulations requiring certification of every new service.

FedRAMP review often takes 12-18 months for a new product and 4-12 months for a Significant Change Request (SCR). These timelines are too lengthy given the velocity of change in the software industry, where updates are often pushed on a weekly basis. Consequently, the Joint Authorization Board is only able to approve 12 new services each year. FedRAMP only has 320 services authorized, and yet, CSPs have thousands of commercially available third-party services. The resulting delay between FedRAMP approval and simultaneous commercial innovation widens the gap between commercially available products and services and what is available to government. This circumstance has created a de facto forked codebase for the commercial and government implementations of the same products, which both increases costs and delivers an inferior service than that which is commercially available.

Instead of requiring new certifications that delay and degrade the quality of the service that can be provided, we recommend the Government and CSPs should agree on fundamental gating criteria which, if met, will allow updates to previously certified systems for government customers. This change will speed up government adoption of cloud services, which is the purpose of FedRAMP, while maintaining Government control over fundamental security features. Various reviews and checkpoints can be established and automated during the software development lifecycle to provide the Government with confidence that adequate security and validation checks are performed at every stage of the process. Although this fix is reasonable over the short-term, a long-term solution will rest on a transition, to the maximum extent practicable, to the commercial cloud and away from government-unique clouds to enable the government to leverage maximally the full security and feature benefits of shared infrastructure.

Software is always changing. As CSPs modernize their tech stacks, pay down technical debt, and release new features, they make changes to the codebases. In the past, the SCR process has entailed inconsistent determinations about what constitutes a major change. FedRAMP should provide a clear sense of decision making, escalation paths, and timelines for how CSPs will submit SCRs in compliance with the new approval paradigms imagined in this memorandum.

Lead an information security program grounded in technical expertise and risk management.

We support the evolution of the program and are excited to see it scale. To speed up the approval process, FedRAMP should shift to a data-driven approach where CSPs provide information in an automated way. OMB should outline a process wherein CSPs engage in automated, continuous

monitoring of key security compliance controls, capable of providing relevant reports to the government in a dashboard, or through published machine-readable formats for ingestion into government compliance reporting systems. Moving to a risk-based, continuous monitoring model rather than a single point-in-time certification model also allows the government to validate, in real time, whether current systems are performing as intended. The government would be able to leverage these automated, continuing monitoring sources for continuously assessing the state of security requirements and ensuring compliance.

GSA's FY23 appropriations increased funding for the Federal Citizen Services Fund (FCSF) which funds Project Management Office (PMO) operations. OMB's vision for the program, however, entails a level of service provision that exceeds current funding levels. Given the goals of increasing the total amount of authorized CSPs and thus the continuous monitoring workload that is placed on the PMO, the Coalition would like to see explicit long-term funding goals for the program to maintain a consistent level of service and monitoring across the CSP landscape.

When discussing the expansion of authorization types, the memorandum mentions "expert-led 'red-team' assessments to be conducted on any CSP at any point during or following the authorization process." We would like to learn more about OMB's desire to harmonize these procedures with existing continuous monitoring and incident disclosure processes. How would this sort of program square with existing and proposed regulatory requirements in the Federal Acquisition Regulation (FAR)? What criteria would be utilized to trigger a red team review? We are curious about what additional CSP resourcing would be required for this new workstream versus existing processes, such as those with third party auditors.

The Government should consider expanding the role of the FedRAMP PMO to be the central point of contract for continuous monitoring. It is inefficient for the CSP to provide the same information to multiple agencies, and to coordinate multiple meetings with different agencies. The concept of a joint continuous monitoring review makes sense, but there appears to be little appetite from individual agencies to coordinate and manage joint agency continuous monitoring sessions.

Rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures.

To achieve the original goals of FedRAMP, *i.e.*, to accelerate the adoption of cloud services by federal agencies, the government should establish one, uniform Provisional Authority to Operate (P-ATO) standard. The current situation, with multiple, differing, non-mission-distinguishing criteria for FedRAMP authorization depending on the agency, is antithetical to OMB and Congressional intent. The FedRAMP Director and commercial suppliers should work together closely to ensure that any agreed-upon controls are commercially available, feasible, and/or sufficient to address the government's security concerns.

The new pathways for authorization recognize the reality of agency-specific and cross-cutting Government needs. There is a commercial market for Software as a Service (SaaS) solutions that can be critical to satisfying an agency's mission, oftentimes designed specifically for recurring public sector use cases, providing the best solution for the agency. To allow for quicker and more

effective adoption and usage of these pathways, OMB should develop mechanisms to allow for continued learning about new offerings that could use those pathways to become part of the options or choices agencies can make to integrate into their infrastructure. These pathways also should incentivize the use of fair software licensing to enable application portability so that an agency component can choose the solution that best suits their needs, allowing other components within the same agency to make different choices without worrying about the underlying vendor getting in the way of that choice.

The memorandum imagines a larger CSP authorizing program wherein more employees from Federal agencies will be engaged in authorizing cloud services than are today. We recommend OMB clarify (or delegate to GSA to explain) what certification and continuing professional education requirements will be required of FedRAMP PMO staff and Joint Agency authorizing personnel to maintain their skills with the fast pace of innovation. The Department of Defense (DOD) currently maintains a list of approved certifications across Manual 8570 and Manual 8140.03. The Coalition encourages OMB and GSA to consider methods of creating a standard technical training baseline for employees engaged in cloud accreditation to achieve programmatic goals.

Joint agency approvals should be objective, automated, and left to the agencies that know their own risk. In the presumably rare instances where the FedRAMP PMO disagrees with the agencies, OMB should have in place an appeal or reconsideration process for denied authorizations, along with clear documentation that explains the criteria, procedures, timelines, and escalation paths for appeal processes. This documentation should outline possible results and solutions to ensure fair and uniform application of decisions. By so doing, OMB will help to make appeal processes more standardized, automated, and fast.

To implement the FedRAMP Act presumption of adequacy and encourage reciprocity among agencies, OMB should specify clear and objective criteria for the FedRAMP director to determine when additional resources, scrutiny, or authorization work are necessary. Doing so will ensure transparency for customers and providers seeking authorization. It also would demonstrate FedRAMP's commitment to empowering agencies rather than strictly enforcing compliance.

Streamline processes through automation.

The memo’s guidance to the PMO to coordinate with the Board and the Cybersecurity and Infrastructure Security Agency (CISA) to create a new framework for continuous monitoring is a welcome and exciting opportunity to reduce inefficiencies and improve cloud security. CSPs currently invest considerable resources into compliance with continuous monitoring and ongoing authorization in support of maintaining a security authorization that meets FedRAMP continuous monitoring requirements. The Coalition requests clarity on decision-making, escalations, and tension between automation and risk assessment mechanisms. As continuous monitoring evolves, it presents an important opportunity to harmonize with just-in-time security directives, such as CISA’s Binding Operational and Emergency Directives (BODs and EDs), as well as Federal Acquisition Security Council (FASC) exclusion orders.

It is essential that FedRAMP establish an automated process for the intake and use of industry-standard security assessments and reviews. Automating the intake and processing of machine-readable security documentation and other relevant artifacts will reduce the burden on program participants and increase the speed of implementing cloud solutions in a timely manner.

Several Coalition members can submit content in the Open Security Controls Assessment Language (OSCAL) format today. Without API endpoints, however, it is of limited use and still requires manual processes for the Government to ingest. GSA has made progress in driving adoption of OSCAL, and we encourage additional near-term investment in this area to make Continuous Authority to Operate (ATO) a reality, coupled with a sustained focus on automating many parts of the FedRAMP program to reduce manual, repetitive procedures and to increase staff focus on security.

Harmonize compliance frameworks to enable cloud adoption at scale.

Due to their status as government contractors and operators of Federal Information Systems (FIS), CSPs are on the receiving end of differing requests for information, patching, and disclosures. FedRAMP should reduce regulatory incongruence and increase harmonization across the Federal information technology (IT) compliance ecosystem. One specific way is to consider the effect CISA's promulgation of BODs and EDs has on the existing continuous monitoring framework. We recommend OMB consider ways in which BODs and EDs can be woven into existing FedRAMP compliance mechanisms, as opposed to requiring net-new workflows that are not always aligned with risk from the PMO's perspective.

Furthermore, validation of new cryptographic modules under the Federal Information Processing Standards (FIPS) 140 program has not kept pace with private sector best practices. This lag has caused a bifurcation, discussed above, between innovative commercial solutions and those sold to government agencies. The FIPS program has not kept pace with innovations, and its lack of approvals for cryptographic modules meaningfully impacts Federal cybersecurity. The Coalition recommends an increase in funding and sustained management oversight specifically for the FIPS program to speed up the process of module approval. FedRAMP also should consider additional flexibility in how/when it requires FIPS 140-3 compliance across its baselines.

Other comments from Coalition Members

The role and authority of the Technical Advisory Group (TAG) is unclear and may overlap with the FedRAMP Board. Consider whether the TAG is necessary.

For FedRAMP to succeed, there needs to be an increase in the quality and quantity of Third-Party Assessment Organizations.

Conclusion

The Coalition urges the OMB to adhere to the timelines in the proposed memorandum, including development of a plan to encourage the transition of Federal agencies away from the use of government-specific cloud infrastructure. The Coalition hopes you find these comments useful

and thanks you for your time and consideration. If you have any questions, I may be reached at (202) 315-1053 or rwaldron@thecgp.org.

Regards,

Roger Waldron
President