October 1, 2024

Peter Waterman
Director
FedRAMP Program Management Office
Technology Transformation Services
The Federal Acquisition Service
The General Services Administration
1800 E Street, NW
Washington, DC

Dear Director Waterman:

Congratulations on your new role and we look forward to collaborating with you to improve the FedRAMP program. We appreciate your leadership as this program significantly affects the enterprise software industry and consequently both our government and business customers. We know that there have been a number of changes coming into the program, and we are excited about the opportunity to help improve it. We appreciate the emphasis that FedRAMP is placing on these four core areas of 1) Customer Experience; 2) Cybersecurity Leadership; 3) Scaling the Trusted Market; and 4) Program Effectiveness. On behalf of the members of BSA | The Software Alliance, I would like to draw your attention to several important concerns that our members have raised about the current FedRAMP program. We ask that you consider the following specific recommendations designed to better improve this important program.

BSA is the leading trade association representing the global enterprise software and technology industry.[1] Digital transformation, and the software that enables it, is essential to businesses of all sizes and in every industry. Our members provide cutting-edge cloud services, data analytics, manufacturing and infrastructure tools, and other digital capabilities to help businesses modernize and grow.

1 *BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.*

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

We want to raise your attention to three areas of concern; 1) Continued Uncertainty for JAB-Prioritized Authorizations; 2) Length of PMO Review; and 3) Vague Requirements:

**Continued Uncertainty for JAB-Prioritized Authorizations**

In the weeks preceding release of M-24-15 *Modernizing the Federal Risk and Authorization Management Program*, the FedRAMP PMO worked closely with JAB-prioritized cloud service providers (CSPs) to complete work on pending JAB authorization packages. FedRAMP offered to either partner these CSPs with one or more agencies to complete an agency authorization, or to work directly with the CSPs to provide a FedRAMP program authorization in the short term. FedRAMP confirmed the latter commitment publicly in an August 12, 2024, blog entry, stating, "In the short term, the FedRAMP team will work with a limited number of CSPs originally prioritized by the JAB, who do not have an immediate agency partner, to issue a program authorization."

Despite these assurances, FedRAMP began notifying JAB-prioritized CSPs in September 2024 that FedRAMP would be unable to provide program authorizations in the short term. We have heard reports that some CSPs who have been working toward a JAB authorization for nearly two years, who now face the tough choice of potentially restarting the authorization process with an agency sponsor, or waiting for FedRAMP to develop and implement new processes for the program authorization pathway. Waiting an additional 18 months, or more, for FedRAMP to develop, define, and implement a new program authorization pathway, when CSPs have already demonstrated compliance with the requisite security controls, seems untenable. It also unnecessarily delays the availability of needed cybersecurity services to federal networks.

We strongly suggest that FedRAMP leverage the security verification work already done by the CSPs and the PMO under the JAB process to offer these CSPs an alternative pathway to authorization over the short term. M-24-15 appears to provide access to such a pathway via the temporary or pilot authorization option. Given the considerable time and resources already invested by the government and its industry partners under the JAB authorization pathway, we urge you to prioritize the development and begin implementation of this pathway as soon as possible.

**Twenty-Four Week PMO Review**

BSA recognizes that the FedRAMP organization is looking to create a process that balances cybersecurity and speed to bring additional cloud resources to the federal government. As technology moves quickly to the cloud and further, cloud technology is needed to update outdated systems.

However, BSA has received numerous member concerns about the length of time for PMO reviews that have been communicated. Companies have spent months to years working

with their authorizing agency and an independent auditor (3PAO) to get their documents ready for PMO review. Given the nature of FedRAMP authorization, and the presumption of adequacy of the ATO process, a 24-week PMO review seems to be too onerous and unnecessarily duplicative for this process. The goal for the PMO review is to provide a quality review of an agency's work rather than redoing the work. Ultimately, the FedRAMP process functions as a risk management tool rather than eliminating all risk. That is the partnership between the agency user and the cloud service provider.

Some agencies have proposed a review time of 30 days for the PMO. This could be the goal for the updated PMO process. In order to meet this goal, we recommend that FedRAMP hire additional contractors to expedite the review process and eliminate the current backlog. Ultimately, FedRAMP should have a public review period that enumerates the length of time that it is taking for the PMO to complete their review. This information will allow for companies to make the business decision if participating in FedRAMP is worth the expense and time that is currently involved.

It is our understanding that the process will be shortened in the future, but the concern is present now. We suggest that there be two different paths between PMO reviews. The first be a review of the agency authorizations and the second would focus on PMO-originating authorizations. The first should not take 24-weeks for a review as another agency and 3PAO have already audited the work. We ask that the FedRAMP PMO publicly detail how they will reduce the wait times, the new updated wait times, and the length of time that it will take to improve this process in the next month.

**Vague requirements from the PMO**

FedRAMP is engaged to make the process smooth between the Cloud Service Providers, the PMO and the 3PAOs, but there are opportunities for improved clarity on requirements to increase authorization speed. BSA has learned that rework of submitted documents happens frequently, and there seems to be a disconnect between what the FedRAMP team wants versus what the authorizing agency wants. It is not clear what is the "right way" to meet the requirements. There seems to be a lack of clarity on the specific guidance issued by the PMO, so that companies must go back for clarity from either the agency sponsor, the 3PAO or the PMO. Without a precise example or standard to follow or a level of detail that is expected (e.g., a requirement for multi-factor authentication or FIPS-140 validated cryptography), it causes rework by the tri-parties pursuing the FedRAMP authorization. Clear requirements and communication between the PMO and the CSPs that do not allow for varying interpretation will eliminate the delay that is occurring presently.

BSA stands ready to work with you to improve this program and we would welcome any further engagement as this process continues to move forward. We want this program to be successful and look forward to finding paths to bringing additional cloud technology to the federal government.

Sincerely,

Craig Albright
Senior Vice President
US Government Relations

Cc:
United States House Committee on Oversight and Accountability
United States Senate Committee on Homeland Security & Governmental Affairs
Office of the Federal Chief Information Officer at the Office of Management and Budget, Executive Office of the President