December 20, 2023

Clare Martorana
Federal Chief Information Officer
Office of Management Budget
725 17th Street, NW
Suite 50001
Washington, DC 20503

Re: BSA Comments on Office of Management and Budget (OMB) Request for Comments on Updated Guidance for Modernizing the Federal Risk Authorization Management Program (FedRAMP)

Dear Ms. Martorana:

BSA | The Software Alliance appreciates the opportunity to provide comments on the Office of Management and Budget (OMB)'s Request for Comments on Updated Guidance for Modernizing the Federal Risk Authorization Management Program (FedRAMP).

BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy.[2] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, and collaboration software. BSA members are on the leading edge of providing AI-enabled products and services. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible use of AI.

BSA appreciates FedRAMP's goal of using "commercial cloud services by Federal agencies is itself a major cybersecurity benefit" [3], but we believe that significant work needs to be done to achieve it. FedRAMP has failed to reduce the duplication

[1] Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.
[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.
[3] *See* the Office of Management and Budget, Modernizing the Federal Risk Authorization Management Program (FedRAMP), *available at* https://www.cio.gov/assets/files/resources/FedRAMP-updated-draft-guidance-2023.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

of efforts by commercial cloud providers to provide services to the federal government as it often takes 12 to 18 months for a new product review and 4 to12 months for a Significant Change Request. Current technology updates are pushed out on a quarterly, or more frequent basis, so there is a conflict between the commercial market and the ability for the federal government to obtain current software. BSA believes that security and speed can reasonably co-exist and looks forward to making suggestions to the memo to assist with this goal.

We recommend revising several aspects of the OMB memo to ensure OMB, agencies, and the FedRAMP PMO can better implement this program. Specifically, BSA recommends that OMB:

I. Continue FedRAMP authorizations
II. Ensure clarity and feedback
III. Create consistency surrounding certifications
IV. Further refine process restructuring
V. Clarify cloud service
VI. Create regulatory harmonization and
VII. Support improved FedRAMP processes

I. Continue FedRAMP authorizations

Cloud service providers under active review for a Joint Authorization Board (JAB) authorization are already experiencing uncertainty and delays as a result of the current authorization restructure proposal. Further delays in pending authorizations reduce cloud service availability and security to the federal government and may result in added costs if assessment activities are duplicated under a new authorization process. Recognizing the significant investment of time, effort, and resources by the government, its partner assessment organizations, and Cloud Service Providers (CSP) under the existing JAB authorization process, we seek a commitment from the FedRAMP PMO that it will bring existing FedRAMP Prioritized, Ready, or In-Process packages through to a Preliminary Authorization to Operate prior to adoption of a new authorization structure, without further delay, and in accordance with existing milestones and timelines for the JAB authorization process.

BSA also suggests extending the transition periods to ensure their efficacy. There is concern that the timelines are going to be challenging to meet and could postpone current ongoing FedRAMP processing.

II. Ensure clarity and feedback

BSA recommends that OMB provide more clarity and detail on its roles and responsibilities in relation to FedRAMP, as well as the mechanisms and processes for communication and collaboration with the FedRAMP PMO and other stakeholders. To aid in this outreach, BSA also recommends that OMB include a Frequently Asked Questions section as an addendum to the final memorandum, which has been used in prior OMB documents.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

BSA also recommends that OMB include the Federal Secure Cloud Advisory Committee (FASC) in the Guidance. In addition, BSA requests that OMB specify the FASC's roles and responsibilities, as well as the procedures for its establishment, membership, meetings, and reporting so that there is clarity for all interested parties.

BSA recommends that the OMB Guidance clarify the Technical Advisory Group's (TAG) role and scope of work as an advisory body, as well as delineate the expectations and deliverables for its members.

III. Create consistency surrounding certifications

As stated in the Public Meeting on November 15, 2023, BSA strongly supports OMB's belief that the federal government should use the same products as the private sector. We urge OMB to provide clear guidance to agencies to allow for private sector innovations to be used throughout the federal government with a streamlined process for consistent certifications across the environment. The current process can involve several steps, which delays the use of technology while not increasing security.

BSA urges OMB to authorize agency CIOs to presume FedRAMP certification adequacy across the federal government by providing a uniform authority to operate (ATO) standard. Multiple, differing criteria for FedRAMP authorization across agencies do not promote the acceleration of cloud adoption. OMB should provide more guidance while requiring consistent ATO acceptance on how agencies demonstrate their security needs beyond FedRAMP authorizations. This action allows the FedRAMP certification to become the standard across the federal IT environment, rather than one additional hurdle to federal cloud acceptance.

BSA also encourages the acceptance of widely recognized standards such as SOC, PCI, and CMMC so that federal agencies have the opportunity to use the most current IT software and cloud services. BSA suggests that the guidance encourage FedRAMP to actively collaborate with industry stakeholders to develop clear guidelines on how these external assessments can be seamlessly integrated into the FedRAMP authorization process. This will allow for faster access to more modern technologies to be used across the federal government.

BSA asks OMB to collaborate with agencies and industry stakeholders to define the criteria for expediting authorizations. BSA is also grateful that OMB recognizes the value of newer industry practices, like Artificial Intelligence, and is looking forward to partnering with OMB on developing ways to increasing adoption.

IV. Further refine process restructuring

BSA asks for clarification on how the restructuring of the JAB will affect the current role and function of the JAB, and how it will impact the authorization process for CSPs. This is a new authorization authority which should allow for multiple agencies to get and use current cloud software, infrastructure and platforms quickly. As it is new, additional guidance for industry would help as the process begins.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

In the same vein, BSA asks for clarification on the mention of "any other types of Authorizations" by OMB in its memo on joint agency authorization. Additional information on the types of authorization that are being considered would be appreciated so that industry can work with the PMO to have the cloud software, infrastructure, and platform out quickly.

Finally, as the authorization and review process is expanded, BSA would like to understand how this expansion will be funded so that the goal of speed can be met. Further information on funding of this important project is needed so that reviews can move forward quickly.

BSA asks for additional clarification on FedRAMP's documentation reviews of all authorization types and when red team assessments are warranted. The proposed requirements include an initial and potential ongoing obligation for “expert-led red teaming”[4]. We urge OMB to revise the memo’s approach to expert or external red teaming. Testing is an important part of ensuring appropriate security and functionality, but involving external entities in such testing can create concerns around access to trade secrets or other proprietary information. Encouraging contractor-led internal testing avoids requirements for companies to disclose this sensitive information to third parties, while shifting the risk to the vendor rather than a third party.

BSA also requests that additional information regarding “special review of existing FedRAMP authorizations (regardless of authorization type)”[5] be more clearly detailed under the Memorandum. BSA asks that OMB encourage the FedRAMP PMO to provide additional, narrowly tailored guidance on the criteria triggering these special reviews. Without further detail, companies are unable to manage the potential of arbitrary reviews rather than those that are detailed under a prescribed triggering schema.

BSA encourages OMB to provide guidance that encourages FedRAMP to create formal escalation processes for CSPs to provide next steps if an authorization process is delayed or denied. Organizations need to have a path to correct any potential issues so that commercial cloud software, platform, and infrastructure can be deployed across the government quickly.

BSA applauds OMB's efforts to promote automation of FedRAMP security assessments and continuous monitoring. It also applauds the use of “industry standard security assessments and reviews.”[6] This will help to make the process more predictable, while also producing consistent data standards across the effort. To further speed up the approval process, FedRAMP should shift to a data driven approach for continuous monitoring. CSPs should deliver systems with 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 dashboard model rather than a single point-in-time certification model

[4] Id at 7.
[5] Id at 11.
[6] Id at 4.

also allows the government to validate in real time whether current systems are performing as intended. Once that dashboard shows required data feeds are active and security requirements are met, the product should be approved for sale in the marketplace. This dashboard should then be used for continuously assessing the state of security requirements.

To assist in this effort, BSA encourages OMB to promote the use of AI to support automation goals. BSA suggests that OMB work with GSA and other agencies to implement AI risk management programs based in the NIST AI Risk Management Framework, which can anchor processes for overseeing and governing AI applications in the federal government. The NIST Framework can assist as FedRAMP develops its use of the technology while also overseeing the rapid incorporation of AI in the federal government.

BSA recommends that OMB provide clear guidance and timelines for Open Security Controls Assessment Language (OSCAL) adoption, as well as facilitate collaboration and feedback among the OSCAL developers and users. In addition, BSA encourages OMB to provide clear explanations on the expected benefits and challenges of implementing automation across different authorization types as this may impact businesses as they work through the new processes.

BSA notes that CSPs are constantly updating and improving their products and services. In the commercial market, these updates can be pushed to the customer immediately. However, in the government market, current regulations require certification of each “significant change” which leads to the ongoing, inefficient, and less secure reality of a bifurcated codebase for the same product. BSA would like to know if advanced notice from CSPs of upcoming security-relevant changes would be required under the new construct or will there be fewer formal mechanisms to share information. Specifically, will the introduction of new operating systems to the already FedRAMP-authorized inventory require approval via a Significant Change Request form from the FedRAMP Director? Or could the notice be communicated informally by CSPs through advance notice channels to speed the delivery of the newer service? If the goal of the new memorandum mirrors the White House’s efforts to speed the delivery of software across the government, BSA suggests that the advance notice channel would be more effective.

An alternative to the advance notice channel would be that the government and CSPs agree on a fundamental gating criteria which, if met, will allow updates to previously certified systems for government customers. This change will speed government adoption of cloud services while maintaining government control over fundamental security features. Various reviews and checkpoints can be established and automated during the software development lifestyle to provide the government with confidence that adequate security and validation checks are performed at every stage of the process.

Finally, given that both GSA and NIST have significant roles in the FedRAMP process, BSA requests that both the FedRAMP PMO and NIST have adequate staffing and funds to conduct the work on this program. Currently, GSA’s Federal Acquisition Service has three staff to work through the program. With the increase in

the types of authorizations, there needs to be a concurrent increase in staffing to support the new process to help aid in further adoption and review of company products.

NIST is currently tasked with reviewing underlying NIST standards, assessing and updating standards and guidelines to meet the current marketplace, monitoring the private sector, and developing machine-readable standards. This technology is evolving quickly, and the work of NIST is vital to provide consistent standards across the federal government. Funding is crucial for the work and staff to conduct its mission effectively.

V. Clarify cloud service

BSA recommends that OMB make statutory considerations and more flexible risk management approaches to accommodate diverse and evolving cloud services. Cloud services can range from private to hybrid to fully commercial and the full range of needs to be contemplated in the guidance.

BSA asks for clarity surrounding cloud services that are outside the scope of FedRAMP. BSA requests additional guidance regarding the status of essential services supporting various platforms, such as Windows Update and App Stores.

VI. Create regulatory harmonization

The OMB memo includes recommendations to agencies for AI procurement. We strongly encourage OMB to ensure the memo takes account of other ongoing regulatory actions that intersect with issues at the center of the OMB memo.

We recommend the memo acknowledge the need for OMB to work towards harmonizing the range of draft regulations and guidance that are currently out for industry comment and review. These include the OMB's recently closed memo on Artificial Intelligence" Moreover, the Federal Acquisitions Council is considering three rules for which the comment period was extended to February 2, 2024 (FAR-2021-0017 Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing; FAR-2021-0019 Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems), and the last FAR rule (FAR- 2023 – 06 Federal Acquisition Regulation: Implementation of Federal acquisition Supply Chain Security Act (FASCASA) Orders).

We urge OMB to consult with stakeholders including industry to look at these changes in concert, as the multiple regulations will need a coordinated approach to advancing AI innovation. With the number of changes in the regulatory environments for IT and specifically, AI, thoughtful analysis on the interplay between these rules and regulations can help the federal government better achieve its stated goals.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

VII. Support improved FedRAMP processes

BSA is pleased with some of the proposed changes to the FedRAMP construct and wanted to share this support with you. In particular, BSA supports the initiative to offer multiple authorization structures as this will assist technologies to come into the federal market quickly at a scale that works for the specific instances. To promote this goal, BSA suggests reviewing the incentives and flexibility for CSPs in concert with the existing considerations for Agencies to make sure that all parties are adequately incentivized for the cultural change.

BSA also appreciates the emphasis on continuous monitoring in the OMB Guidance for FedRAMP. Continuous monitoring enables enterprises to effectively manage their cyber risks, which evolve as malicious actors develop new ways to try to exploit vulnerabilities.

Finally, BSA appreciates the emphatic support for commercial cloud technologies, both in the memo and in the public forum. The US government has a long tradition and standing policy of using commercial software to fulfill its needs. Commercial product software, including Commercial off-the-shelf Software (COTS), allows Federal agencies to have state-of-the-art solutions. It provides reliability, scalability, and flexibility so that agencies can nimbly respond to unexpected or changing conditions, to meet the current need. BSA looks forward to assisting OMB as FedRAMP continues to help agencies use commercial cloud technology across the federal government.

* * *

BSA appreciates the opportunity to provide comments on the OMB memo and would be happy to serve as a resource as you continue to develop your approach to these issues.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org