December 22, 2023

Clare Martorana
Federal Chief Information Officer
Office of Management and Budget
1650 Pennsylvania Avenue, NW
Washington, DC 20502

Re: Request for Comments on Updated Guidance for Modernizing the Federal Risk Authorization Management Program (FedRAMP); Docket # OMB–2023–0021
Document number 2023-23839

The Cloud Service Providers-Advisory Board (CSP-AB) welcomes the updated Guidance from the Office of Management and Budget (OMB) regarding the vision, scope and structure of the Federal Risk Authorization Management Program (FedRAMP).

The CSP-AB represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

Collectively, our members hold over 700 ATOs across all service models and impact levels. As such, we recognize the considerable change that industry and cloud service technology has undergone since the inception of FedRAMP in 2011. Updating the operation of FedRAMP is crucial to ensuring that the Federal government develops more agile, effective, and innovative standards which reflect the realities of the cloud ecosystem.

Additionally, we applaud the OMB for revising its timetable to ensure a robust and transparent consultation process with industry. We are excited about the possibilities that FedRAMP reform could hold, and urge OMB to be bold but judicious as it evolves the program to ensure Cloud Service Providers (CSPs) with existing authorizations are not penalized by the new changes and that velocity of federal cloud adoption does not slow down.

We have provided some specific areas below where we encourage OMB to give further consideration. We have also included some more detailed feedback in Annex 1.

Overarching comments

FedRAMP review often takes 12-18 months for a new product and 4-12 months for a Significant Change Request (SCR). These timelines are far too lengthy in the software industry, where updates are pushed on a quarterly – or even more frequent – basis. The resulting delay between FedRAMP approval and simultaneous commercial innovation widens the gap between commercially available products and services and what is available to the government. This 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.

The FedRAMP process is not only lengthy but costly to both CSPs and the government. Receiving an ATO or approval for an SCR costs hundreds of thousands of dollars and both processes are largely paper-based exercises. The FedRAMP program office is only able to approve 12 new services each year. For this reason, FedRAMP has only 320 services authorized[1]. For perspective, AWS's marketplace has over 10,000 third-party services and Oracle's cloud marketplace has over 3,000.

It is partly for this reason that we are encouraged and excited by the observation OMB made that "[t]he Federal Government benefits most from the investment, security, maintenance, and rapid feature development that commercial cloud providers must give to their core products to succeed in the marketplace." Leveraging commercial cloud enables federal agencies to benefit from commercial economies of scale, commercial innovation, and commercial best practices, all of which support agency mission delivery and produce better outcomes for the broader USG and public. This commercial approach is consistent with the decades-long trend in acquisition law and the practical trend toward greater use of commercial offerings that meet government standards.

FedRAMP vision

We note that OMB intends to create a presumption of adequacy baseline in the FedRAMP program in order to support multiple authorization structures. That "presumption of adequacy" has long been a key aspect of the FedRAMP program's purpose to "certify once, reuse many times," and while this presumption is statutorily authorized in the FedRAMP Authorization Act[2] , it is not clear if this presumption would apply to CSPs reusing other CSP authorizations such as a joint-agency authorized Cloud Service Provider (CSP) using a single-agency authorized CSP. We would welcome additional guidance on this point.

The background discussion of the memorandum highlights an important and often overlooked consideration: "Federal agencies all have finite resources to dedicate to cybersecurity, and must focus those resources where they matter most. The use of commercial cloud services by Federal agencies is itself a major cybersecurity benefit, freeing up resources that would otherwise have to be dedicated to operating and maintaining in-house infrastructure." Increased Federal use of shared, commercial infrastructure will, over time, result in lower cloud computing costs for more modern, secure, and feature-rich infrastructure. Given OMB's leadership role in

[1] https://marketplace.fedramp.gov/products
[2] https://www.congress.gov/117/bills/hr7776/BILLS-117hr7776enr.pdf#page=1055

driving IT modernization budget increases across the USG, it is appropriate that this memorandum guide agencies toward more cost-effective, long-term solutions. At the same time, it is important to note that those savings are *not* generated by security short-cuts, but by adopting shared infrastructure that is *more* secure because it incorporates the best security practices of the commercial marketplace, with its economies of scale. In like manner, CSPs and the public benefit when CSPs incorporate more public sector approaches to cybersecurity and risk management. We urge OMB, GSA, the FedRAMP Program Management Office (PMO), and agency Chief Information Officers and Chief Information Security Officers to ensure this perspective and direction translate into timely action.

When considering new authorization structures, we ask OMB to harmonize such structures with guidance issued by the US Department of Defense (DOD) on ATO reciprocity, and include DOD authorizations among the baselines being considered. We also encourage OMB to ensure FedRAMP's charter includes outreach to educate government users on their own security responsibilities related to the use of cloud products as well as new offerings and how they can help to achieve enterprise-specific and USG-wide goals without lowering the appropriately high bar set by FedRAMP. This would provide an opportunity for industry and government to learn about and share ways in which FedRAMP controls can keep pace with other public sector compliance programs, the threat environment, and modern advances in security.

The FedRAMP Authorization Process

Authorization is the backbone of FedRAMP, so minimizing CSP burden and ensuring a robust standard while maximizing efficiency and effectiveness is crucial. The introduction of multiple FedRAMP authorizations, such as single-agency, joint-agency, and program, reflects a sophisticated understanding of agency-specific and cross-cutting government-wide needs. OMB's decision to allow a program-level authorization for cloud services without a specified agency sponsor demonstrates an innovative, responsible approach to helping agencies identify IT solutions that can provide enterprise-specific and government-wide security, resiliency, interoperability, and economic benefits. While we agree with the overarching goal of the proposed process, we believe additional clarity and details would be helpful in achieving this vision. In particular:

- Per the way the memorandum is drafted, an existing Joint Authorization Board (JAB) authorization appears to be more closely aligned with the Program Authorization and not a Joint Agency Authorization. This is due to the fact that JAB authorization is granted with heavy collaboration with the JAB and the Program Management Office (PMO) and not individual agencies. We would welcome additional rationale from OMB on this point, and ideally enhanced guidance in the memorandum about the responsibilities of agencies and CSPs as they move from a JAB to a joint agency authorization model.
- It is not clear which agencies or program owners CSPs will continue to work with on authorization maintenance if existing JAB authorizations are transitioning to

Joint-Agency Authorizations. We recommend additional clarity in the memorandum around single-threaded ownership and responsibilities in the Joint Agency Authorization paradigm.

- The CSP-AB has concerns over how and where the Department of Defense (DoD) and the Defense Information Systems Agency (DISA) fit into the authorization and maintenance phases, particularly given responsibility is shifting from the FedRAMP JAB/Board to Agencies/PMO. Since DISA sits on the JAB, the JAB has been a seamless way for CSPs to collaborate with DISA. We recommend OMB's revision of the memorandum create an explicit role for the DoD in order to ensure for future interoperability across defense and civilian system authorizations.
- We are also concerned that even more CSPs will have to duplicate efforts when it comes to maintaining authorizations in a joint agency authorization framework. For example, will submitting a Significant Change Request (SCR) require two separate workstreams - one workstream to the PMO and a separate workstream to DISA? If so, this could introduce further delays or inconsistencies if one workstream experiences delays in approval and would thus disincentivize CSPs from pursuing those authorizations if they become more bureaucratic and burdensome.
- It is not clear how disagreements between agencies on acceptable risks or SCRs will be resolved. The current Technical Reviewer workflow in the JAB is not perfect, but it is a known process. We would welcome additional clarity from OMB on how decisions will be made between agencies. To the extent practicable, providing the rationale behind decisions made can help CSPs better prepare future submissions. Additionally, a notification letter and debriefing akin to that introduced in the acquisition process by INFORM 2.0 would prove valuable in improving the quality of information shared and ultimate satisfaction with the adjudication process.

Continuous Monitoring (ConMon)

While we appreciate OMB's consideration of ConMon issues, this Guidance should expand to address risk management deficiency triggers.

To improve the approval process, FedRAMP should shift to a data-driven approach where CSPs provide data to a centralized dashboard. 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 continuous monitoring data 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. 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.

For example, static limits on risk triggers do not take into account the nature of common vulnerability exposure (CVE) occurrences in large scale systems and run directly counter to the principles of agility and flexibility to which the Guidance states to adhere. As new CVEs are discovered constantly, one can think of the rate of CVE detections as a function of the number of dependencies a system has. In other words, the more dependencies a system has, the more likely it will be impacted by a given CVE. Therefore, the number of CVE detections is not a function of the effectiveness of a system's controls but rather simply reflects the size/complexity of the system.

Shift from the current static triggers model to a more adaptive model that will consider the authorization status of hyperscale CSPs while still accommodating the risk profiles of smaller CSPs with existing baselines. We recommend changes to the Continuous Monitoring Performance Management Guide such that the risk management deficiency triggers or acceptable thresholds should be based on a tiered model based on hosts and service provider models (Saas, PaaS and IaaS).

CSPs are constantly updating and improving their products and services. In the commercial market, these updates can be pushed to the customer immediately; in the government market, regulations require certification of each “significant change”, which leads to the ongoing, inefficient, and less secure reality of a “forked” codebase for the same product.

Instead of requiring new certifications that delay and degrade the quality of the service that can be provided, 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 government adoption of cloud services – 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 lifestyle to provide the government with confidence that adequate security and validation checks are performed at every stage of the process.

The CSP-AB has previously submitted via FedRAMP a detailed proposal for a tiered approach to risk triggers; we attach that paper to this submission for your consideration.

Potential to Increase Access to Authorization Pathways for CSPs

Our members applaud the memorandum’s goal of increasing access to FedRAMP authorizations, particularly to SaaS vendors. The ability for a CSP to receive a PMO authorization without an agency sponsor would be a paradigm shift for the program, and one that we believe will open doors to new entrants to the federal cloud marketplace. Should the idea be correctly implemented, it can increase innovation in public sector technology by getting more cloud solutions into more agency users’ hands.

Common P-ATO Standard Across All Agencies

We are concerned about the variety of requirements being imposed by different agencies. Therefore we would request a common P-ATO standard. To achieve the original goals of FedRAMP – to safely accelerate the adoption of cloud products and services by federal agencies – the government should establish one uniform P-ATO standard. The current state of affairs— with multiple, differing criteria for FedRAMP authorization depending on the agency— is antithetical to OMB and Congressional intent. The FedRAMP Director and commercial suppliers should work closely together to ensure that any agreed-upon controls are commercially available, feasible, and sufficient to address the government's security concerns.

Evolving Federal Information Processing Standards (FIPS) Compliance.

CSP-AB has been a longtime advocate of reforms to the Federal Information Processing Standards 140.[3] Validation of new cryptographic modules under the FIPS 140 program has lagged behind private sector best practices for many years. This has caused a bifurcation 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. We encourage OMB to use the FedRAMP reform process to consider the introduction of new processes or procedures at NIST that will shorten the time from submission through validation, thereby providing a sustainable solution to the current backlog.

Training and Certifications for Government Personnel

The memo imagines a larger CSP authorizing program wherein additional employees from Federal agencies will be engaged in authorizing cloud services than currently do today. 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 CSP-AB encourages OMB and GSA to consider methods of creating a standard technical training baseline for its employees engaged in cloud accreditation to achieve programmatic goals.

Operationalizing Red Team Reviews

The memorandum mentions "expert-led 'red-team' assessments that can be conducted on any cloud provider at any point during or following the authorization process." The CSP-AB would like to learn more about what OMB and GSA have in mind for this sort of program: would it be over and above existing ConMon and incident disclosure procedures? How would such a program square with existing and proposed regulatory requirements in the FAR (see section above on Regulatory Harmonization)? What decision criteria would be utilized to trigger a red

[3] FIPS For the Future, Cloud Service Providers-Advisory Board and Coalfire, July 2023, https://www.csp-ab.com/_files/ugd/67ea70_96f8cb9502e84eaa953fd48af1b9631d.pdf

team review? Further, what would CSP support for such a review look like vis-à-vis existing processes such as those with third party auditors? We understand the value some red teaming can bring. At the same time, if not designed properly, additional exercises could impose significant burdens on internal CSP infrastructure and system availability and could risk the exposure of sensitive customer data. Any such teaming exercise should be carefully tailored to yield substantially more benefits than the burdens imposed on CSPs and should be tightly aligned with the controls outlined in NIST SP 800-53.

Additional items for consideration

Accreditation for third-party assessment organizations (3PAOs) is not mentioned. We would welcome additional clarity on whether 3PAOs will continue to be part of the FedRAMP process and which FedRAMP body will accredit them.

The final version of this memorandum might also provide instruction to Federal agencies concerning future use of the antecedent FedRAMP Standard Contract Language template[4], and it might task GSA with developing an updated version that reflects the policies in this memorandum.

We encourage OMB to leverage and strengthen the important contributions of this memorandum by incorporating them in a new cross-agency priority goal ("CAP" goal) on IT modernization and management. The President's Management Agenda ("PMA"), which organizes and articulates those goals, provides an excellent opportunity to echo these themes and commitments.

We also welcome further detail for CSPs already with an authorization separate from the commercial infrastructure, and whether such a CSP would be able to utilize this authorization.

As a closing observation, we support the OMB in its admirable aim of promoting enhanced security and agility. However, while stakeholders during this consultative process have acknowledged the issue, the Guidance does not directly contemplate the higher cost that is borne by those wishing to serve US Government environments. It also does not specifically address the increased budget and resources that will be needed by FedRAMP to implement and maintain this enhanced standard.

It is critical that government and CSPs develop new approaches to FedRAMP that account for the increasing pace of innovation. The current, retroactive FedRAMP review process will continue to fail to scale with increased demand and increased functionality. The government and CSPs must work together to reframe the existing structures to achieve Congress's original

4 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/FedRAMP_Standard_Contractual_Clauses_062712_0.pdf

intent in creating FedRAMP: accelerate the adoption of non-duplicative cloud products and services across the federal government.

We thank OMB for conducting a public comment period for this draft memorandum. We would welcome a future opportunity to speak to your team about our feedback in the coming weeks.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Provider - Advisory Board

lnavaratnam@csp-ab.com

Annex 1 - Additional detailed feedback

Guidance Section	Comment #	Comments
Section III, Scope of FedRAMP	1	With the expanding footprint of hybrid cloud solutions, we welcome additional clarity on whether FedRAMP's scope of review will extend to encompass hybrid cloud solutions that function both on-premise and in cloud-based environments moving forward.
	2	*"Agencies must obtain a FedRAMP authorization when operating an information system within this scope."* Previously, Cloud Providers were the only ones required to get FedRAMP Authorizations (P-ATOs from the JAB or Agency Authorizations from a Sponsoring Agency). Agencies issued the final ATOs for a system. We welcome additional clarity from OMB in relation to the declaration that "*Agencies must obtain a FedRAMP authorization when operating an information system within this scope.*"
Section IV, FedRAMP Authorization Process	3	*"FedRAMP will establish a set of criteria for expediting the authorization of packages submitted by interested agencies with demonstrated mature authorization processes."* The long queue for PMO Agency ATO package reviews is a pain point for CSPs. The current wait time for the PMO to start the review is 20+ weeks. We would like to see the review process streamlined and communications improved regarding visibility into position or movement in the queue.
	4	Joint-agency authorization We welcome additional clarity on how the FedRAMP Board and FedRAMP PMO will proactively assist with this type of authorizations and support Agency Cohorts.

	5	*"Existing JAB P-ATOs at the time of the issuance of this memorandum will be automatically designated as a joint agency FedRAMP authorizations."* We are concerned that in cases where a JAB P-ATO cloud service offer has dozens of Agency customers, it will be very challenging in practice for a large number of federal agencies to co-manage a Joint Agency ATO.
	6	Types of Authorization We welcome additional clarity on how FedRAMP will select these CSPs for program authorization and what the criteria for selection would be. We also note that there is little information regarding 'any other type of authorization'. We welcome additional consultative detail in due course from OMB and/or PMO as appropriate.
	7	Red Team Assessments We welcome additional clarity on the practical application of red team assessments, including how and when a cloud service offer would be subjected to a red team assessment, who will make up the red team (e.g. FedRAMP 3PAOs), whether certain CSP personnel will be notified, how assessments will overlap or contrast with NIST AI red team assessment standards set forth by EO 14110, and who will bear the cost of red team assessments.
	8	We encourage OMB and GSA to collaborate with the Department of Defense (DoD) to streamline the authorization process between FedRAMP and the DoD SRG, with the aim of enhancing efficiency and promoting cloud adoption across the Federal Government. Eliminating a DoD component from the authorization process could potentially impede the authorization of cloud services at the IL4 and IL5 security levels.
	9	We would like to better understand the approach that will be adopted for ConMon in the context of joint-agency FedRAMP authorizations. Several CSPs shifted to JAB authorizations in response to the inconsistencies in ConMon requirements within a multi-agency authorization framework.

	10	We would like to better understand if there are any intentions to introduce legislation mandating agencies to establish a cloud authorization group. This group would facilitate the management of the expected surge in cloud service offerings, aligning with the outlined authorization models.
	11	*1. "... if a given cloud product or service has a FedRAMP authorization of any kind, the Act requires that agencies must presume the security assessment documented in the authorization package is adequate for their use in issuing an authorization to operate, and that neither additional security controls nor additional assessments of those controls are required....An agency may overcome this presumption if the agency determines that it has a "demonstrable need" for security requirements beyond those reflected in the FedRAMP authorization package, or that the information in the existing package is "wholly or substantially deficient for the purposes of performing an authorization"* ; *2. "The FedRAMP Director remains responsible for deciding whether an agency's additional security needs merit devoting additional FedRAMP resources and conducting additional FedRAMP authorization work to support a revised package. "* In the past, it was assumed that FedRAMP security requirements served as a minimum baseline, and agencies would frequently tailor and add additional security according to their unique agency needs for a system to receive an ATO. We request additional clarity on how OMB intends to enforce the requirement for *"demonstrable need"* so that Government Agencies cannot impose additional agency specific security requirements, or require additional assessments, beyond those specified by FedRAMP on a CSP. Item 2, above, limits the FedRAMP director's ability to determine additional "*FedRAMP resources"* and not general CSP resources.
	12	At present, it is very difficult for Cloud Providers to find an agency to sponsor an authorization. Agency CIOs and CISOs are often unwilling to sponsor Cloud Providers due to lack of familiarity with FedRAMP. Instead, most Agencies require that Cloud Providers already have a FedRAMP authorization prior to using the service. However, the current JAB process is bottlenecked and the Agency review process requires a Sponsor. This "chicken/egg" problem means that Cloud Providers cannot even apply for authorization, and increased costs to the government because it is unable to use cloud services that are not authorized.

		We request additional clarity on whether OMB will formally expand the role of FedRAMP to educate and encourage Senior Agency officials, such as at the CIOs and CISOs level, to sponsor Cloud Providers for authorization. It is also requested that the role of agencies (Section VII (d) pages 15/16) be updated to request that they actively engage in sponsoring Cloud Providers for FedRAMP authorization.
	13	*"FedRAMP reviews are not limited to reviewing documentation, and may direct that intensive, expert-led "red team" assessments be conducted on any cloud provider at any point during or following the authorization process."* 1. Does OMB intend that "red team" assessments be conducted in addition to, or instead of the Security Assessments done by the 3PAOs? 2. Although OMB states that FedRAMP may direct that these assessments be conducted, OMB does not direct FedRAMP to establish the criteria for these additional intensive assessments. It is requested that OMB direct FedRAMP establish clear guidance and criteria for these red-team assessments. This includes (but is not limited to) selection criteria for Cloud Providers, clarification of roles and responsibilities for all parties (including the CSP, 3PAO, FedRAMP, etc.), selection criteria for the "expert assessors", frequency of assessments, requirements for remediations, whether the findings will be publicized (or not), etc. 3. These additional expert led "red team "assessments are very expensive. Who would be required to pay for these assessments - the CSP or the government? 4. There are more than 300 FedRAMP authorized services at present. How does OMB intend for FedRAMP to conduct these intensive, expert-led "red-team" assessments at scale across the even larger numbers (in the future) of Cloud Providers, and the diverse kinds of cloud providers?
	14	*"Cloud providers are increasingly using complex architectures and encryption schemes to guarantee confidentiality and integrity, and FedRAMP must be able to validate that relevant implementations are reasonable and appear to work as intended."* Does OMB intend that FedRAMP conduct validations of the encryption implementation instead of, or in addition to, those required by the NIST CMVP? If these will be conducted in addition to those required by the CMVP, who will pay for the cost of these assessments?

	15	*"... leverage the use of threat information to prioritize control selection and implementation" based on "... a threat-based analysis, produced in collaboration with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA)...".* At present, CISA's threat intelligence and analysis is limited to distribution within the government only. Will OMB direct that FedRAMP share this threat intelligence and analysis with Cloud Providers so that the Cloud Providers can appropriately support FedRAMP in its mission to defend against these threats?
Section V. Automation and Efficiency	16	We would like to better understand how this interacts with the GSA deadline for establishing means of automation for security assessments by Dec. 23, 2023.
	17	We appreciate OMB's specific inclusion of control inheritance artifacts among the scope of information to be provided in a machine-readable format. We encourage OMB to view control inheritance as a critical mechanism for lowering barriers to entry and supporting innovation among software developers, including small businesses and startups, who design products which run in FedRAMPed environments.
	18	We encourage FedRAMP, in due course, to publish which external audit frameworks and associated evidence from those external certifications it would consider acceptable. We encourage FedRAMP to consider including DOD authorizations and ISO27001 in this category.
	19	It is recommended that OMB and FedRAMP collaborate with service and software vendors to establish a standard that promotes the implementation of compliant configurations by default by CSPs. These configurations should enable the generation of consistent evidence to demonstrate both point-in-time and continuous compliance.
	20	*"Additionally, many existing cloud offerings have implemented or received certifications for external security frameworks. Performing an assessment of such a framework each time a product that uses it goes through the FedRAMP process unnecessarily slows the adoption of such cloud products and services by the Federal Government. Therefore, FedRAMP will establish standards for accepting external cloud security frameworks and certifications, based on its assessment of relevant risks and the needs of Federal agencies. This will include leveraging external security control assessments and evaluations in lieu of newly performed assessments ..."*

		FedRAMP has historically not accepted reciprocity even internally between systems that have received JAB vs. Agency authorizations. So it is appreciated that the OMB requests that FedRAMP should implement reciprocity between different security assessment frameworks. However, it is requested that OMB underscore this request by requesting that FedRAMP engage the 3PAOs, Cloud Providers, A2LA, FS-CAC and industry bodies for this.
Section VI, Continuous Monitoring	21	It is recommended that the PMO create a framework that incorporates real-time threat intelligence feeds, integrating these metrics into the CVSS scoring and associated threat modeling. This will aid in assessing whether a change introduces substantial risks to the authorization boundary, facilitating a transition towards a more quantitative risk assessment approach, as opposed to a qualitative one.
	22	We welcome additional clarity on whether there is a plan to establish a structured review and acceptance procedure for continuous monitoring activities. Previously, agencies have had diverse requests regarding the contents of continuous monitoring deliverables, resulting in confusion and increased administrative burden.
	23	We welcome additional clarity on what the specific criteria will be that would necessitate a "special review" of existing FedRAMP authorizations conducted by the FedRAMP PMO. It is advisable to establish clear criteria to prevent any perception of bias.
	24	*"To increase integrity and further trust in the FedRAMP program, FedRAMP should leverage government-wide tools and best-practices to enhance its monitoring efforts. Specifically, FedRAMP must ensure that it uses, to the greatest extent possible, CISA's capabilities and shares relevant data and tools for monitoring FedRAMP's products and services."* Based on the above statement, is the intention for FedRAMP to leverage CDM tooling and processes for Cloud Providers?
	25	OMB encourages FedRAMP to create a framework to improve Continuous Monitoring. It is recommended that OMB encourages FedRAMP to create this framework with input from the CSP community and the FS-CAC.

	26	*"For all FedRAMP authorized products and services, the FedRAMP PMO will provide a certain standard level of continuous monitoring support to authorizing agencies. The FedRAMP PMO will set this standard level of monitoring support by analyzing and identifying the highest impact controls for ensuring security of FedRAMP products and services."* It is recommended that OMB encourage FedRAMP to engage with the CSP community to establish these standards. A CSP offering a large IaaS with millions of nodes (for network, storage, and compute) would have different ConMon requirements than a CSP with a small SaaS offering.
	27	We welcome additional clarity on what will trigger a special review of an existing FedRAMP authorization, the scope of a special review including type of testing performed, and what advanced notice will be provided to CSPs prior to a special review.
Section VII Roles and Responsibilities	28	*"Proactively engage with the commercial cloud sector, to represent the priorities of the Federal agency community and maintain awareness of contemporary technology and security practices;"* We welcome enhanced engagement with the GSA and FedRAMP PMO. We encourage FedRAMP to consider hosting more events on site at GSA with cloud service providers and 3PAOs, as such forums have been highly effective in the past.
	29	The FedRAMP Board We encourage OMB, in the spirit of transparency, and in due course, to make membership of the Board and the technical advisory group public.
	30	*"The FedRAMP Board consists of up to seven senior officials or experts from agencies that are appointed by OMB in consultation with GSA. The Board must include at least one representative from each of GSA, DHS, and the Department of Defense, and will include representation from other agencies as determined by OMB. The FedRAMP Board members must possess technical expertise in cloud, cyber, privacy, risk management, and other competencies identified by OMB, in consultation with GSA"* One of the major issues with the current composition of the FedRAMP JAB (with the three CIOs from DHS, DOD and GSA) is that their FedRAMP responsibilities are a small part of their overall job role. They currently meet twice a year to

		attempt to address very complex national cyber issues, which is insufficient to meet the overwhelming needs of the total FedRAMP program. Furthermore, neither they nor their designated Technical Representatives (TRs) are exclusively dedicated to FedRAMP tasks. It is recommended that OMB require that the seven senior officials from the agencies above be exclusively dedicated to FedRAMP and its related activities.
	31	It is recommended that OMB add an additional responsibility for the Board to engage with the broader FedRAMP stakeholders outside of government including Cloud Providers, 3PAOs, and industry experts.
General	32	We encourage the FedRAMP PMO, in collaboration with the CSP and 3PAO community, to establish a Continuous Assessment Framework (CAF) as an optional alternative to the traditional “Annual Assessment” framework in order to mitigate audit fatigue and reduce risk to CSPs’ system security boundaries and their customers by identifying and thereby remediating findings sooner. Traditionally, RMF expects the system to be audited on an annual basis. While this is a significant improvement over the legacy framework where audits were conducted every three years, it still leaves a significant gap that the monthly ConMon process does not address. This is an opportunity to bridge the gap, reducing risk to the system and to customers while improving service delivery and new service release outcomes. A strategic partnership would be required between the CSP, Authorizing Official, and 3PAO. Tactically, the CSP and 3PAO will need to collaborate on a coordinated compliance program plan detailing the execution of the Continuous Assessment Framework. Strategically, the CSP and 3PAO need to collaborate and coordinate with the AO to obtain stakeholder buy-in and approval of the new cadence and coordinated compliance program plan to show that it meets all of the compliance baseline policies, improves the systems security posture, and reduces risk while maintaining or reducing the AO’s level of effort. If the CSP distributes the annual controls throughout the year, the audit activities become a standard operating procedure i.e., a week-to-week and month-to-month routine activities which is less disruptive and requires less time from supporting teams as well as being paced at a predictable and manageable cadence.

		By assessing a handful of controls each month, the CSP will identify findings sooner and ultimately have more time to remediate them in comparison to the traditional annual assessment, which usually identifies dozens of findings at one time. In the typical annual assessment, the CSP only has a week or two to remediate as many as they can before the findings count against them in the SAR and a surge of findings are often added to the POA&M. At that point, the CSP has a higher number of findings that need to be remediated in the same 30, 90, and 180 day timeframe as they would if those findings were identified a few at a time throughout the year. Additional benefits of a CAF would include allowing for a more scalable service release cadence of new functionality to be continuously added to a CSP through the SCR process while maintaining existing compliance authorizations i.e., faster time to market for authorized CSP functionality and services; scaling to meet increasing compliance obligations and to use compliance as a competitive advantage i.e., by complying with all of the expected security baselines such as FedRAMP P-ATO, SOC2 and DoD IL5 PA; increasing the productivity of CSP's delivery teams by coordinating audit activities to reduce the time spent in audits; and, of course, reducing risk to CSP's system security boundary and tenants by identifying and thereby remediating findings sooner.