April 30, 2021

The Honorable Katy Kale
Administrator
U.S. General Services Administration
Office of the Administrator
1800 F St. NW
Washington, DC 20405

The Honorable Sonny Hashmi
Commissioner
U.S. General Services Administration
Federal Acquisition Service
1800 F St. NW
Washington, DC 20405

The Honorable V. David Zvenyach
Commissioner
U.S. General Services Administration
Technology Transformation Services
1800 F St. NW
Washington, DC 20405

IA Recommends FedRAMP Reforms In Light Of New Funding For The Federal Citizen Services Fund

Dear Administrator Kale, Commissioner Hashmi, and Commissioner Zvenyach:

Internet Association (IA) represents the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our member companies are global leaders in the drive to develop lower cost, more secure, and innovative digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

On behalf of our members, I thank the entire GSA team for having prioritized the securing and modernization of legacy information technology (IT) infrastructure as well as the streamlining of business processes surrounding compliance. Having developed many of the tools and applications that serve as the core of the modern digital government experience, IA member companies have also been some of the earliest and most frequent users of the services provided by the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO) and the FedRAMP program itself.

Considering the importance of cloud-based services in the government's resilience during the COVID-19 pandemic and the widespread adoption that will continue at an even greater pace going forward,[1] it is imperative that the federal government is able to securely adopt the new and emerging technologies being developed on cloud-based platforms or as cloud-based services. Furthermore, the adoption of these new technologies must happen at a similar, if not faster pace, to meet evolving mission needs and keep the nation's networks secure.[2]

[1] *See* Gartner, Inc., "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021" (November 17, 2020)

[2] *See* White House, "President Biden Announces American Rescue Plan"; see "Modernize federal

GSA should prioritize additional funding and support for the FedRAMP PMO to deliver on long-requested program changes.

Following the recent appropriation of $150 million for the Federal Citizen Service Fund (FCSF), there is a real opportunity to build the foundation that will allow FedRAMP to achieve its mission of being the "do once, use many times" accreditation group for federal use of cloud technology, an essential component of any federal government modernization effort. However, this can only be achieved by addressing persistent challenges limiting the program's ability to meet its core mission.

To that end, we respectfully offer the five recommendations listed below, which are based on years of experience and familiarity with the day-to-day operations and long-term, strategic goals of the FedRAMP PMO, the Joint Authorization Board (JAB), third-party audit organizations (3PAOs), the National Institute of Standards and Technology (NIST), and similar accreditation-related entities across the public sector in the United States:

1. Evolve FedRAMP to focus on delivering adaptable and scalable cyber risk reduction for the entire U.S. government
2. Scale the FedRAMP federal team and empower staff to streamline processes to focus on core mission objectives
3. Empower 3PAOs to provide continuous monitoring, enabling the FedRAMP team to focus on high priority issues and long-term goals
4. Prioritize enhanced, clear escalation processes to improve transparency and outcome consistency
5. Commit to meaningful, consistent industry engagement to continuously mature the program

As is described below, addressing these areas will enable the FedRAMP PMO to focus their resources on strategic and scalable cyber risk reduction goals rather than their existing remit, which is narrowly focused on compliance. This is especially important as the FedRAMP PMO staff consists of only four full-time employees (FTEs), one Director, and part-time help from the Assistant Commissioner — they will need all the support that can be made available to them in order to manage and meet the security objectives and digital transformation needs of the nation.

It is the current funding for the FSCF that will provide the FedRAMP team with the resources they require to ultimately be an enabler for modernization and security across the entire nation rather than a potential blocker to both. We are at an inflection point where the FedRAMP PMO can deliver a significant and substantial change to the way in which agencies and departments enhance their security and stability, and by executing on these recommendations, detailed below, the FedRAMP program will be able to better serve its ultimate customer - the U.S. government.

Recommendation 1: Evolve FedRAMP to focus on delivering adaptable and scalable cyber risk reduction for the entire U.S. government

Cloud security has evolved significantly since FedRAMP was first started in 2011[3], but even with about

information technology to protect against future cyber attacks." (January 20, 2021)

[3] *See* White House, "Security Authorization of Information Systems in Cloud Computing Environments"

300 products at various stages of the authorization process, the FedRAMP PMO and the requirements of the program itself have - worryingly - remained almost unchanged. As a result, the PMO itself suffers in its ability to execute on its vision to adopt a modern approach to the strategic management of cyber risk reduction in a consistent and scalable manner to support federal agencies. Rather, the program is being focused on a set of compliance activities, some of which increase cost to both government and industry without meaningfully enhancing security. Fortunately, there are two key ways that would address this issue and reduce risk:

1. Create outcome-oriented security goals
2. Improve the deviation request process

Create outcome-oriented security goals

The program should move towards a model that incentivizes and rewards success in the reduction of cyber risk by meeting the determinate security goals, rather than checking off a series of boxes. For instance, the Significant Change Request process is too broad: there should be a delineation between the level of effort of proof, evidence, and documentation required based on the actual risk. Currently, all significant change documentation and the timeline for approval (3-6 months) is the same regardless of severity. Upgrading this business process to a more risk-related approach will save the government precious resources and would be a helpful way to evolve the PMO's operations. Additionally, FedRAMP should provide 3PAOs the ability to meet with, discuss, and memorialize specific control implementations with CSPs, as some of these implementations may actually exceed desired outcomes and should provide preferable considerations (i.e., faster authorization times, streamlined approvals for changes) for the CSP.

Improve the deviation request process

The PMO should work to improve its internal workflows - especially those pertaining to the submission and comment flow of deviation requests - in order to allow for effective automation. For instance, this process currently requires the approval of three separate personnel across the agency, regardless of the risk profile of the deviation. Additionally, the adoption of Service Level Agreements (SLAs) for responses to submissions as well as a risk-based approach to review and approval of deviation requests will ensure the federal government obtains the latest and most secure modernization technology in a predictable and timely fashion.

Recommendation 2: Scale the FedRAMP federal team and empower staff to streamline processes to focus on core mission objectives

As the benefits of cloud-native applications are felt and seen throughout the public sector, the number of CSPs that will apply for FedRAMP certification will continue to grow and become simply unsustainable if FedRAMP does not scale appropriately.[4] This will result in the PMO being unable to accommodate the demand of government organizations for various cloud-based products and services. Considering the length of time the federal hiring process takes, the PMO must be incentivized to increase its capacity by streamlining processes in order to keep up with the likely volume of near-term and long-term

(December 8, 2011)

[4] *See* Government Accountability Office, "Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked", GAO-19-58, https://www.gao.gov/assets/gao-19-58.pdf (April 4, 2019)

certification applications. General Services Administration (GSA) and the Technology Transformation Services (TTS) should spend their new appropriated dollars on paying down the program management technical debt that has accumulated throughout the past decade and empower the PMO government staff to scale the process. Three opportunities that can be very impactful and leveraged quickly include:

1. Automating the reporting and authorization process
2. Providing applicants with real-time visibility
3. Scalable and extensible compliance documentation

Deploy automated reporting and authorization process to enhance real-time visibility

Considering the administrative burden associated with reporting placed on both industry and federal staff, the existing manual process has already outlived its usefulness and is unsustainable. TTS should use the influx of funding into the FCSF to establish a more transparent process that scales and meets the needs of both government and industry stakeholders. Developing a dashboard that will centralize and coordinate critical FedRAMP JAB activities would help automate the authorization process, submission of Plan of Action and Milestones (POA&Ms), and with permission sets, allowing CSPs to input and update those authorization requests and POA&Ms. Additionally, it can act as a clearinghouse for information related to cyber risk reduction across the entire U.S. government and serve as a window into those insights for the Federal Chief Information Officer (CIO) and Chief Information Security Officer (CISO), among other stakeholders. The new funding can be used to ensure that the PMO builds a useful tool to enable its work to really scale, building on the developments that have arisen since this idea was first submitted to FedRAMP in response to the Ideation Challenge that took place in 2019.[5]

Real-time visibility and automation in the authorization process

With FedRAMP authorizations taking anywhere from 4 to 18 months, appropriately planning for projects that are mission-critical requires transparency into the process. Based on our estimation, there are four FTEs inside the PMO and four to eight FTEs as the primary technical reviewers and technical reviewer leads inside the FedRAMP JAB. Though they are supporting the program and undoubtedly pushing authorizations through as fast as possible, the limited resources available in terms of funding and personnel are making the limitations of such a small team with an incredibly large mandate felt across the U.S. government. The program could also use the centralized dashboard recommended above to provide essential information to the users of the FedRAMP process, especially for those CSPs who have numerous applications in various stages, furthering the ability of the PMO to support a larger number of cloud-based services. Additionally, appropriately utilizing automation throughout the authorization process will further reduce authorization time. At the same time, FedRAMP should publicize its jurisdiction (unclassified, Outside Continental United States (OCONUS) regions) and limitations (i.e., hardware in customer's physical environment) so that CSPs have consistent public guidance on what's applicable for FedRAMP and avoid an unnecessary investment of time and resources in pursuing an authorization for out of scope cloud service.

Integrate scalable and extensible compliance documentation to reduce manual and time-intensive work

There are numerous plans and documentation required with FedRAMP as well as Federal Information Security Modernization Act (FISMA) compliance, the development of which accounts for the majority of the resources CSPs must spend to create and support FedRAMP authorization to operate (ATO)

[5] *See* Challenge.gov, "The FedRAMP Ideation Challenge: Shape how government performs cloud security authorizations.", https://www.challenge.gov/challenge/the-fedramp-ideation-challenge/ (ended August 22, 2019)

packages. Whether through increased implementation of the Open Security Controls Assessment Language (OSCAL)[6], the use of machine-readable formats to provide improved processing of documentation, updating documentation standards and processing will be crucial to scaling PMO's operations. We recommend TTS prioritize hiring headcount to support the operationalization of scalable compliance frameworks and invest in building out an extensive system to work with CSPs of all sizes, bringing the dream of increased automation to fruition. This is especially important for the continuous monitoring process, where the manual aspects of the status quo approach have proven problematic.[7]

Recommendation 3: Empower 3PAOs to provide continuous monitoring, enabling the FedRAMP team to focus on high priority issues and long-term goals

Approval times and breakdowns in applications can be attributed to the turnover in staff at the PMO and JAB, causing longer than necessary processing timelines as well as lower approval rates. More to the point, the increase in turnaround time has effectively prevented FedRAMP from fulfilling its promise of enabling wider U.S. government cyber risk reduction and IT modernization efforts. With high turnover rates among federal government staff, the FedRAMP PMO and JAB should take advantage of the institutional knowledge that exists within 3PAOs and their interactions with CSPs. This would also provide the federal government with the added benefit of having a trusted partner able to make better risk-based decisions that will streamline and improve the program itself. Empowerment of 3PAOs would be most impactful in three particular areas:

1. Documenting and approving significant changes
2. Sharing vulnerability data
3. Reviewing deviation requests

Leverage 3PAOs to document and approve significant changes

The length of time and the amount of documentation required to add new features or provide updates to authorized applications and those within the process of achieving FedRAMP certification results in the government failing to take advantage of the latest technology available. This is particularly impactful to agency and department missions that are unable to adapt and meet the needs of their end-users. By allowing 3PAOs, using a defined set of criteria, to help determine the risk level of the change, future submissions of significant change reports (SCRs) can be narrowed down to only those with certain levels of risk.

Further reduce risk by limiting access to sensitive vulnerability information

The current requirement to share complete and unredacted vulnerability data, some of the most sensitive technical data about a CSP, unnecessarily exposes FedRAMP, the JAB, and the CSPs themselves to a great degree of risk. Allowing 3PAOs, many of whom already have physical access to CSP facilities as well as technical access to CSP infrastructure, to provide independent verification of this data will mitigate the risk of access to or exfiltration from a singular source in the event of an incident.

Review deviation requests using a risk-based approach

The review of deviation requests is slow because they are performed manually, and often without a

[6] *See* NIST, OSCAL: the Open Security Controls Assessment Language (last accessed March 24, 2021)
[7] *See* Government Accountability Office, "Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed", GAO-20-126, https://www.gao.gov/products/gao-20-126 (December 12, 2019)

risk-based approach as the driving guiding force, which has negative downstream impacts on POA&Ms and other methods of communicating risks. Utilizing a prioritization system that will provide 3PAOs the ability to assist the JAB by reviewing Low and Moderate risk requests while leaving High risk requests to the JAB itself would simultaneously improve results and increase capacity.

Recommendation 4: Prioritize enhanced, clear escalation processes to improve transparency and outcome consistency

Industry often feels beholden to the PMO and JAB's decisions to the point that many are afraid to escalate issues. The lack of formality in the dispute resolution process, and issues related to PMO and JAB staff declining to honor agreements made by former staff members has magnified unnecessary delays. In the event of a disagreement between the JAB and a CSP, a clear mechanism or feedback loop that will allow for an appeal of the disputed decision coupled with an SLA for all stakeholders involved would introduce some much needed clarity and consistency to the process. Additionally, a historical record of decisions will ensure future disputes are resolved as early as possible, allowing all resources to be focused on securing applications rather than dealing with disagreements. TTS should leverage its new funding to design and implement an escalation process so that government employees are able to make risk-based calculations as needed.

Recommendation 5: Commit to meaningful, consistent industry engagement to continuously mature the program

As the PMO has evolved, so has its mechanisms for seeking feedback from CSPs. A lack of formality in the industry engagement process as well as issues related to providing feedback prior to the implementation of policy or rule changes are hampering the ability of the program to address new issues. More consistent, transparent, and formalized means of engagement will ensure FedRAMP and industry collaboration are combined to create the safest and most reliable certification of cloud security available to the public sector. For example, the PMO held a “JAB Connect” event in 2019 as well as a “Container Safety” discussion in 2020, but they lacked any follow-up or constancy. Those events were steps in the right direction, but they did not yield any changes or new work streams. We recommend that TTS prioritize funding for the PMO to communicate and run consistent processes for any major changes to reporting, compliance, and program processes.

Considering the experience and knowledge gained by CSPs on the “front lines” of cybersecurity work, the ability to share information and exchange best practices with one another will be critical. Utilizing a process similar to that used by NIST when updating and improving their standards would provide the FedRAMP PMO with the same ability to collaborate with, and build off of the lessons learned by industry. It would also create a symbiotic relationship among key stakeholders that would likely increase security and compliance, while also helping government agencies rapidly evolve and adapt to emerging threats.

With the above in mind, we would appreciate the opportunity to meet with you and your teams to discuss the specific ways that newly allocated funding can be used to help move FedRAMP into its second decade of essential work.

FedRAMP has made great strides since its inception, going from 0 to 100 in six years and jumping from

100 to 200 in just two years.[8] This incredible rate of growth will only continue to increase. As a result, like any program or process, there will always be new circumstances and concerns that will require change to accommodate current needs and requirements. The pandemic, recent infiltration of government infrastructure, and the general sustained progress in terms of the tools and techniques used by the most sophisticated of advanced persistent threats (APTs) are examples of such catalysts.

By achieving the outcomes outlined in our recommendations, we believe that FedRAMP will be able to continue to provide the leadership, guidance, and most importantly, trust, that other government agencies and departments rely on. With continued and meaningful support from GSA leadership and engagement with industry, the opportunities are endless.

We appreciate your time in considering our feedback and look forward to the opportunity to discuss them with you in further detail.

Most sincerely,

Omid Ghaffari-Tabrizi,
Director, Cloud Policy

Cc: Ms. Ashley Mahan
Mr. Brian Conrad
Mr. Zachary Baldwin
Mr. Ryan Hoesing
Ms. Betsy Steele

[8] *See* FedRAMP, "FedRAMP Reaches 200 Authorizations", https://www.fedramp.gov/fedramp-reaches-200-authorizations/ (September 17, 2020)