Written Testimony of Jonathan Berroya
Senior Vice President and General Counsel
Internet Association

Before The House of Representatives Committee on Oversight and Reform
Subcommittee on Government Operations
Hearing on the Federal Risk and Authorization Management Program Reform Act of 2019
July 17, 2019

Chairman Connolly, Ranking Member Meadows, and distinguished members of the Committee, thank you for the opportunity to appear before you today to discuss the Federal Risk and Authorization Management Program Reform Act of 2019. My name is Jonathan Berroya, and I am the Senior Vice President and General Counsel at Internet Association.

Internet Association (IA) represents over 40 of the world's leading internet companies. We support policies that promote and enable internet innovation and are dedicated to advancing public policy solutions that strengthen and protect internet freedom, foster innovation and economic growth, and empower users. Our companies are also global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors.

A bit more about us: the major U.S.-based hyperscale cloud providers are members of Internet Association. We have members that handle a broad range of government data types in their clouds — from publicly available data to the most sensitive national security intelligence. All of our cloud service provider (CSP) members invest a tremendous amount in security and compliance.

Simply put, cloud computing enables on-demand access to shared computing resources, providing critical services to agencies so they can focus less on maintaining infrastructure and more on their mission.[1]

I would like to start by thanking the bill's sponsor, Committee leadership, and their staff for their diligent work on this legislation. All IA cloud vendors are committed to the highest levels of information security, and collectively invest hundreds of millions of dollars in compliance and certifications across both U.S.-based and international assessment frameworks.

[1] GAO-19-58 https://www.gao.gov/assets/700/698236.pdf

Furthermore, our member companies have been working with the public sector for much of the past decade — many well before the creation of the FedRAMP PMO or even the Cloud First policy. We have watched FedRAMP grow from a nascent team in the Office of Citizen Services and Innovative Technology to a productive, although under-resourced, group in the Federal Acquisition Service's Technology Transformation Services.

IA supports the goals of the legislation. Today, we would like to put forward a number of guiding principles that we believe will help ensure the FedRAMP program continue to deliver a value-add to both the government and vendor community supporting it, leading to greater adoption of commercial cloud services government-wide.

Internet Association and its members understand FedRAMP's value and essential function in the federal IT marketplace. Consequently, we have the following four major themes to discuss with the Committee:

- First, we would like to see more reusability of Authority to Operate (ATO) packages once a vendor has received a FedRAMP Joint Authorization Board (JAB) approval via a provisional ATO (P-ATO).
- Second, we would like to ask Congress to allow the program to evolve to keep pace with innovation.
- Third, we would like to see industry have a seat at the table as FedRAMP innovates to stay current.
- Fourth, we believe this program needs more resources in order to assess and accredit the coming wave of cloud products.

I. Solve Underlying Issues With Reusability Of Security Packages And Reuse Of ATOs Across Civilian Agencies

One of the biggest outstanding issues with the current FedRAMP program is the lack of ATO reciprocity across federal agencies, including for vendors who have already received a P-ATO from the JAB. Given the cost of compliance and accreditation, IA would like to see even more ATO reciprocity throughout the executive branch.

While FedRAMP has led to a great deal of control standardization across government, it has been unable to fix the underlying issue: that each CIO must still issue individual authorizations - which is in direct contrast to the "authorize once, reuse many times" mantra that FedRAMP promised at its inception.

We understand and appreciate the importance of FISMA as a law that places the risk acceptance burden for IT systems squarely on the agency CIO's shoulders. However, we would like to ask that the JAB P-ATO become more reusable, with greater CIO trust placed in the JAB and its assessment of the NIST baselines and security controls as opposed to the agency CIO

doing a re-assessment and/or adding unnecessary reviews. Industry would like to ensure the JAB, GSA, and OMB continue to push for increased reuse of security packages and that FedRAMP assessments of relevant security controls are considered sufficient for each agency's relevant FISMA compliance burden.

The 2011 OMB memo that created FedRAMP[2] aimed high when it outlined that ..."[b]y using an agile and flexible framework, FedRAMP will enable the Federal Government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a government-wide scale." We would like to see policy and practice that underscore this idea and allow for greater reuse.

IA believes that government agencies should be encouraged to leverage FedRAMP JAB authorizations to the fullest extent possible versus creating their own. At the same time, agency CIOs should retain the authority to make their own risk-based decisions about cloud services. For this reason, we would like to ensure that FedRAMP continues to serve as the convener and advocate for authorization reuse.

II. Allow For Continued Program Evolution

We support a FedRAMP process that is committed to evolution, and one that aligns with the pace of innovation. The PMO should consider new approaches and techniques for evaluation and monitoring that lower compliance's administrative burden for industry while encouraging reuse throughout government. Industry has noticed and appreciated GSA's commitment to receiving and acting on feedback thus far — and creating steps such as FedRAMP Ready and Low Impact SaaS (LiSaaS) as a direct result of feedback from the ecosystem of CSPs and agency cloud customers.

The FedRAMP program creates efficiencies for the government by enabling common assessments of cloud service providers, which allows a cloud provider to certify once and have that certification shared among the agencies. The result is intended to be a more efficient process than individual agency evaluations, with the ultimate goal of reuse of artifacts. FedRAMP also creates a process for cloud service providers to provide transparency into their operations and empowers agencies to fulfill their responsibilities for systems. As designed, FedRAMP was the first government program to help balance responsibility between government agencies and cloud providers.

IA would like to see that any legislation does not codify more bureaucratic process than necessary, and allows GSA and the PMO to continue making changes and evolving as the market evolves. For instance, we see a not-too-distant future where much of the controls and

[2] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

NIST baselines are audited in a fully automated way with fewer intermediaries, less paperwork, and faster processing. Industry would like to ensure that any legislation would not constrain GSA from changing with the times and implementing automation and innovation into their process.

CSPs are rolling out new services in their private sector cloud marketplaces every day, but the lag time associated with expanding ATO boundaries means that the public sector is falling behind due to bureaucratic processes. Industry would like to see a world where government cloud customers are able to leverage the full benefit of cloud computing while automated, seamless compliance frameworks ensure that government information is safe and secure.

III. Continuous Industry Engagement

IA asks for the creation of an Industry Advisory Board or similar body be created to ensure early, formal, and continuous FedRAMP engagement with industry. We aim for the recognition of industry as a partner and stakeholder to ensure policies are not created in a vacuum. Given that FedRAMP is an essential part of the FedRAMP IT procurement landscape, its decisions and business processes have major financial effects on buying practices of public sector entities across the nation.

Further, we recommend the creation of a formal opportunity for notice and comment on changes to authorization processes and other material issues related to program operation. Judgements and policies established by the FedRAMP program can affect the entire government cloud service provider industry, and we would like to have an ability to submit official comments to the program the same way we can to NIST, the Office of the Federal CIO, or other related federal entities.

IV. More Resources

Considering the program's limited resources including shared budget, we have been continuously impressed with GSA's ability to do so much coordination and stakeholder engagement with so few resources. However, the program has now matured and become an integral part of the federal IT and procurement landscapes. Laws such as a FITARA have underscored the importance of the CIO in purchasing technology in government, which has made CSPs more and more reliant on FedRAMP and its processes to access the federal marketplace.

According to the GAO: each year, the federal government invests approximately $90 billion in IT, with about 75 percent reportedly spent on operating and maintaining existing systems. Many of these systems will be modernized using cloud services, and that means the FedRAMP team and their business processes will become even more essential to the cloud business ecosystem than ever before.

In order to continue serving the growing number of agencies that wish to buy cloud services, as well as the vendors who wish to support them and allow Congress appropriate oversight, FedRAMP needs a separate, delineated budget in order to invest in business process improvement while simultaneously processing authorizations and carrying out its other education functions. We understand that GSA has done the most it can with the Federal Citizen Services Fund (FCSF) over the past decade, but the time has come for FedRAMP to graduate to become a program of record with its own money. FCSF is currently used to fund not only FedRAMP but also USA.gov, Login.gov, Data.gov, and gobierno.gov.[3] These programs are all important to GSA and TTS' mission, but FedRAMP's dominance means that these other programs are also receiving less resources from the shared fund.

We would like to ask for the creation of a separate authorization and funding line for FedRAMP's continued operations as well as adequate funding for JAB teams at each agency. Cloud services are only going to become more important to the public sector, and that means FedRAMP's crucial role is only going to increase. For this reason, we believe that giving GSA the separate, dedicated funds to run this PMO and invest in its future will have lasting positive impacts on both the internet economy and the executive branch for years to come.

Conclusion

In conclusion, I would like to reiterate IA's gratitude for being included in the legislative discussions regarding this bill and for the opportunity to testify here today. The FedRAMP program has evolved a great deal over the years, and the internet industry is looking forward to supporting its continued growth and maturity. We know FedRAMP will be essential to continued adoption of innovative cloud services across the public sector, and IA – along with our members – stands ready to support the committee in helping FedRAMP to succeed. Thank you.

[3] https://www.gsa.gov/about-us/newsroom/congressional-testimony/gsa-fy2018-budget-request