Written Statement of

Ross Nodurft

Executive Director

Alliance for Digital Innovation (ADI)

US Senate Committee on Homeland Security and Governmental Affairs

Roundtable: FedRAMP Reform: Recommendations to Reduce Burden, Enhance Security, and Address Inefficiencies in the Government Cloud Authorization Process

November 30, 2021

Thank you, Chairman Peters, Ranking Member Portman and members of the Committee for holding this roundtable on FedRAMP reform.

My name is Ross Nodurft. I am the Executive Director of the Alliance for Digital Innovation (ADI), a coalition of innovative, commercial companies whose mission is to bring IT modernization and emerging technologies to government. ADI engages with policy makers and thought leaders to break down bureaucratic, institutional, and cultural barriers to change and enable government access to secure, modern technology that can empower a truly digital government.

ADI focuses on four key areas in our federal advocacy efforts – accelerating technology modernization in government, enabling acquisition policies that facilitate greater use of innovative technologies, promoting cybersecurity initiatives to better protect the public and private sectors, and improving the federal government's technology workforce. Each of these areas must work closely with each other to allow for government mission owners and technology providers to partner with industry to build a modern, digital government.

ADI's members include some of the leading technology and professional services providers to the public sector, many of which have gone through the FedRAMP accreditation process or are working to achieve FedRAMP accreditation. These technologies underpin the federal government's modernization efforts and provide the backbone for many agencies' zero trust architectures and plans.

Given our areas of focus, ADI applauds the work that Congress – and the members of this committee – have done to evaluate and craft legislation that can accelerate some of the changes needed to enable secure access to modern and emerging technologies. S. 3099, the *Federal Security Cloud Improvement and Jobs Act of 2021*, and its House companion, H.R. 21, if enacted, would provide stability around the FedRAMP accreditation process and authorize the resources needed to drive many of the reforms called for by the Government Accountability Office (GAO)[1] and Inspector General of the General Services Administration (GSA). [2]. Over the last two years, ADI has expressed its support for codification of FedRAMP. More specifically, ADI has stated and maintains its support for:

- the authorization of additional sustained resources to increase the number of FedRAMP authorizations;
- additional collaboration with industry;
- driving reuse and reciprocity of FedRAMP accreditations across the federal government;
- adoption of automation throughout the FedRAMP process; and
- the market certainty that codification provides for innovative companies seeking to access the federal marketplace.

[1] https://www.gao.gov/assets/gao-20-126.pdf
[2] https://www.oversight.gov/sites/default/files/oig-reports/A170023_1.pdf

There are a few provisions of the *Federal Security Cloud Improvement and Jobs Act of 2021* that I would like to highlight; these provisions will help the FedRAMP program achieve its goals and accelerate its planned improvements.

First, the authorization of $20 million annually for five years represents a good start to fully funding the program. This initial increase will provide much-needed, consistent resourcing to hire additional individuals with the technical skills necessary to review and process authorization applications. These resources, coupled with increased use of automation, can quickly expand the number of provisional authorizations issued by the proposed FedRAMP governance board.

Second, the establishment of the Federal Secure Cloud Advisory Committee has the potential to create a consistent, formalized feedback loop through which industry can partner with GSA and the federal agencies to drive consistent improvements and quickly elevate and adjudicate concerns as they arise. We strongly urge OMB, GSA, and CISA to leverage this body proactively and regularly to accelerate cloud adoption across the federal government.

Finally, codification of the FedRAMP program further underscores the importance of the program while creating market certainty that investment in FedRAMP accreditation will mean something in the public sector marketplace in the future. In addition to adding stability to the program through codification, S. 3099 also reenforces public sector market certainty by driving accreditation package reuse by other agencies.

Resourcing the FedRAMP Program

For much of the past decade, funding for the FedRAMP program has remained flat while the program processed and accredited over 240 cloud services. This program has become an essential part of the federal government's cloud adoption journey and remains integrally important to maintaining high cybersecurity standards. The Biden Administration's Executive Order 14028 on Improving the Nation's Cybersecurity[3] specifically calls out the cloud as an important way to raise the bar on security across public sector entities and identifies several actions that the FedRAMP program needs to take to facilitate secure adoption of cloud services.

However, the program's ability to make those changes and to continue to drive secure cloud adoption is contingent on proper resourcing. A FedRAMP accreditation through either the Joint Authorization Board (JAB) or Agency process requires annual paperwork and re-authorizations as part of the continuous monitoring process. In fact, every time a cloud service provider makes a significant change or update to its cloud service offering,[4] it must submit a change notification form to the FedRAMP program management office (PMO) prior to implementing that change. These real time updates and product improvements are at the core of what makes cloud service offerings more scalable and secure. Yet, each of these changes must be manually adjudicated by FedRAMP. Today, this means that GSA must make a choice between accrediting new cloud services at a faster rate and dealing with the backlog of re-authorizations and change

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] https://www.fedramp.gov/assets/resources/templates/FedRAMP-Significant-Change-Form-Template.pdf

requests from services that were approved during the past ten years. These resourcing choices and trade-offs can be reduced through additional funding.

S. 3099 begins to address these resourcing constraints through an authorization of $20 million per year for five years, which is a good down payment on the process. However, ADI believes that even more funding is necessary to turn FedRAMP into the cloud security accreditation program the federal government needs to facilitate the significant shift to cloud services that the Biden Administration is championing.

Federal Secure Cloud Advisory Committee

A formal industry voice has been missing from the FedRAMP conversation since the very beginning. A public/private sector advisory committee may not have seemed necessary when the program began ten years ago. However, the cache that the FedRAMP brand commands in the federal marketplace coupled with the billions of dollars in annual Federal IT spend make it essential for government and industry to work together to improve the program.

Cloud Service Providers (CSPs) have been reluctant to provide feedback to GSA for fear of jeopardizing their relationships with program management staff and accreditation officials. While the FedRAMP program and GSA have reached out and worked with CSPs on an ad hoc basis, there has not been an official forum to formally identify and collaboratively discuss and address the impact of policy changes. Further, agencies outside of those represented by the JAB have not had an opportunity to shape the FedRAMP process despite being key stakeholders and customers of the provisional authorizations to operate (P-ATOs) granted through the program.

The ability to consistently engage with FedRAMP's key stakeholders can be addressed, in part with additional resources. That said, the direction and formal authorization of the Federal Security Cloud Advisory Committee in S. 3099 will provide essential structure that can facilitate a better understanding of the impact of changes in policy as well as a dedicated forum to discuss programmatic improvements that will maintain or improve security while increasing agency access to secure cloud services and products.

Encouraging Reuse and Reciprocity

The Federal Information Security and Modernization Act (FISMA) of 2014[5] requires every federal department and agency to own its own risk. This incentivizes risk aversion across government authorizing officials and IT leadership. While S. 3099 recognizes the requirements of FISMA, it moves agencies in the right direction by codifying the "presumption of adequacy" of the security assessment that underpins a FedRAMP accreditation. Further, S. 3099 requires agencies to reuse the security assessment package whenever possible. This is an important mandate that will help continue driving private sector investment in the FedRAMP accreditation, since reuse is key to the program's value.

[5] Public Law No: 113-283

ADI members believe that having a security accreditation program that will remain in place across administrations helps companies who are considering the investment in FedRAMP. Reinforcing that investment by driving reuse of a product or service's underlying security package also provides more market incentive to pursue a FedRAMP accreditation.

However, government can go even further by providing meaningful reciprocity across compliance regimes. FedRAMP accreditation is already the foundation for cloud security across the public sector. By underscoring FedRAMP as the gold standard in cloud security and encouraging reciprocity in the public sector marketplace, additional modern and innovative companies can make the business case for investing in the FedRAMP process. The more companies are accredited, the more easily government can move away from legacy technology and embrace secure cloud-based emerging technology.

Authorizing Automation

For the last ten years, the FedRAMP process has relied on manual, paper-based compliance processes to build, assess, update, and review authorization packages. This cumbersome practice has continued to underpin – and often slow down – the accreditation process, even as the use of automation, machine learning, and artificial intelligence has proliferated in other parts of the government. The same manual process also drives the review of any significant change request. These manual reviews quickly consume the resources available to FedRAMP causing additional delays for existing services and preventing new CSPs from moving up in the accreditation queue.

While the GSA and NIST have been working closely on a series of automation procedures, the accreditation process still relies on time-consuming, manual processes. S. 3099 requires GSA to review the automation procedures that are currently being developed and tested and, within a year of enactment, establish a means for automating assessments and reviews. This will mark a pivotal change for the program and free up FedRAMP resources who are overburdened by the current manual processes.

Conclusion

In conclusion, ADI supports the efforts of the committee to invest in and improve the FedRAMP program. We are encouraged by the committee's work on S. 3099 and applaud the bill's efforts to increase funding for the FedRAMP program, create a formal process for industry engagement, increase use of automation across the program, and provide market certainty through codification.

ADI appreciates this opportunity to participate in today's roundtable and share our insights on improving cloud adoption in government. I look forward to any questions you might have.