Schellman & Company, LLC
4010 W Boy Scout Blvd, Suite 600
Tampa, Florida 33607
866.254.0000
www.schellman.com

Subcommittee on Government Operations
Committee on Oversight and Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Re: Post-Hearing Question Response by Douglas Barbin, Principal at Schellman & Company, LLC – a FedRAMP 3PAO

August 13, 2019

Thank you for the opportunity to again share my experience with this subcommittee. This supplemental information is provided in response to the letter dated July 30, 2019 with the below post-hearing questions. As with my testimony, the views I express are my own and should not be construed as reflecting any official position of Schellman.

1. From your perspective, when should a company seek an agency sponsored Federal Risk and Authorization Management Program (FedRAMP) authorization versus a provisional authorization to operate through the Joint Authorization Board (JAB)? Do you envision an instance when a company would seek both?

In my experience, the agency versus JAB decision is based on several factors including but not limited to:

- Authorization timeline for an agency compared to the timeline to apply and go through the JAB Connect application and authorization process;
- Demand and how many potential agency customers the cloud service provider (CSP) will serve in the near term;
- Ability for the CSP's initial agency to handle the initial authorization and ongoing continuous monitoring commitments;
- Desire to be listed as a JAB authorized CSP in the FedRAMP Marketplace; and
- Ability to be a sub-service provider or connected system to CSPs seeking JAB provisional authorization. Under the current requirements, systems that connect to or provide services for JAB authorized systems are generally required to have their own JAB provisional authorization.

Larger cloud providers sometimes maintain a combination of agency and JAB authorizations. Most want to move towards JAB for the above reasons, however

agency authorizations are still more prominent due to limited JAB resources. I see no reason why a CSP would seek and maintain JAB and agency authorizations for the same system.

2: What advice would you give to cloud service providers seeking FedRAMP authorization?

While Schellman's services are limited to independent assessments and not consulting or implementation services, we often counsel clients in such a manner that sets appropriate expectations for the program and the assessment process. This regularly includes discussions with current clients that undergo various commercial compliance assessments such as the AICPA System and Organizational Control (SOC) examinations, Payment Card Industry Data Security Standard (PCI DSS) assessments, ISO 27001 certifications, and US and international privacy assessments.

In these discussions, I typically start with the recognition that FedRAMP is based on the most comprehensive set of cybersecurity requirements a CSP has likely complied with to date, almost always exceeding what the CSP had in place for any of the above commercial compliance frameworks.

The second topic is cost and investment. At the hearing, significant attention was placed on the "cost to attain FedRAMP" some citing more than one million in investment. While accurate, it is important in such an analysis to understand the component costs including:

1. Costs to implement the detailed FedRAMP and NIST control requirements. This may include engineering changes, software development and improvements, as well as process updates of documentation, policies, procedures, and training.
2. Consulting services expenditures to help implement the required controls and produce the necessary documentation for FedRAMP.
3. Independent assessor fees to conduct the initial and ongoing assessments and produce the required deliverables.
4. Ongoing continuous monitoring cost for the CSP to perform scanning, monitoring, and provide regular reports to the agency or JAB.

My experience shows that the organization's preparedness to comply with the detailed FedRAMP requirements has the largest impact on costs.

Third, I regularly promote the FedRAMP Ready program's success in shortening assessment timelines. This program, which tests the top 10% of the FedRAMP controls, including all federal mandates, allows CSPs to have their key controls evaluated early in the journey and serves as a diagnostic first step. As FedRAMP Ready does not require an agency sponsor, it allows for cloud providers to demonstrate preliminary capabilities to the marketplace, aiding them in attracting potential agency sponsors and customers.

Question 3: What improvements would you like to see in FedRAMP?

Expanding on my prepared testimony, the following are additional recommendations for improvement to the FedRAMP program. First, continue building community engagement. Several great ideas were mentioned at the hearing including both the establishment of the Federal Secure Cloud Advisory Committee, inclusive of independent assessors, and FedRAMP advocates at each of the agencies.

Additionally, I recommend that the PMO and JAB develop a more formal process for communicating mandates and interpretive guidance out to key stakeholders. Major control changes or modified control interpretations should include a formal feedback process and a reasonable timeline for implementation. In the past two years, I have seen challenging and complex topics from encryption to the use of external service providers where guidance had to be modified and pushed out to CSPs currently under assessment. Stakeholders understand that cloud technologies change frequently and given notice and the opportunity to collaborate, the CSPs will adapt.

Last, I recommend the JAB continue to evaluate its external services risk and dependencies model. Today, the JAB takes an approach that any services utilized by a JAB authorized CSP must also be JAB authorized. While we understand the rationale, it is worth examining potential impacting services in more detail including:

- Underlying infrastructure as a service providers (e.g. AWS or Microsoft Azure where a software application inherits those controls)
- External services or interconnections where federal data sharing occurs
- External service providers that have security impact on the systems housing federal data within the boundary
- External services utilized for supporting operational functions such as ticketing systems or uptime monitoring that have no access to federal data
- External services that provide reference such as software updates or lookup references such as a service that takes an IP address and determines what country the connection came from
- Corporate services that support the overall CSP but do not necessarily have access to federal data

A consistently executed assessment and agency authorization review should address the above in an equally applied manner. We encourage the JAB to continue to evaluate external services in a manner as detailed as possible evaluating the types of data shared, security impacts, compensating controls, and other compliance frameworks to determine if a particular subservice provider needs to be JAB authorized or if an agency authorization or other validation suffices.

Thank you again for the opportunity to provide feedback to the subcommittee. Schellman will continue to make itself available to the subcommittee for any assistance it can provide.