schellman

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

Introduction and Opening Remarks
By Douglas Barbin, Principal at Schellman & Company, LLC – a FedRAMP 3PAO

Introduction

Good afternoon and thank you Mr. Chairman and respective members of this subcommittee for the opportunity to share my experiences with you today.

My name is Doug Barbin. I am a principal at Schellman & Company, LLC, where I am responsible for leading the firm's FedRAMP practice, along with other cybersecurity assessment offerings.

Schellman is a top 100 CPA firm in the United States and is distinguished from other large CPA firms due to our specialization in cybersecurity, compliance, and certification services. Our clients range from startup firms to publicly traded companies.

In 2012, Schellman became the first CPA firm to become a FedRAMP 3rd Party Assessment Organization (3PAO). Since that time, Schellman has grown to become the second largest provider of FedRAMP assessments. In fact, Schellman has performed three times as many FedRAMP assessments as all other CPA firms combined, including the "Big 4."

I offer my insights today as someone who has conducted more than 4,000 security assessments spanning virtually every widely accepted technology compliance framework or program in the United States as well as several international frameworks. The views I express in this testimony are my own and should not be construed as reflecting any official position of Schellman.

Opening Remarks

As you know, the FedRAMP program was designed with the "audit-once, leverage-many" principle with the goal of reducing the redundancy of federal agencies each conducting their own assessments of vendors.

I believe the FedRAMP program has largely achieved that goal. This model is not new and significant credit should be given to program leadership for their ability to launch and adapt the program in a time-frame significantly shorter than other similar compliance frameworks in the commercial sector.

Based on my personal experience, I have three recommendations for the FedRAMP program as it moves forward.

First and foremost, protect the role of the assessor as the independent finder of fact that facilitates the conversation between the cloud provider and the authorizing body. Some commercial compliance programs have blurred the lines between consultant, assessor, and decision maker. These roles are defined in the FedRAMP program and should continue to be strictly enforced. Independence between the parties should always be maintained in both fact and appearance.

Second, remember that the “R” in FedRAMP stands for Risk. Some commercial compliance frameworks adopt a checklist approach of “all or nothing” compliance. Under these frameworks, achieving security is often secondary to achieving compliance with the letter of the written standard. This concern is even more critical due to the rapid changing nature of cloud technologies.

Third, continue the focus on community engagement. New guidance or requirements should be put out for feedback along with reasonable timeframes for implementation. Additionally, there should be a more streamlined process for cloud providers to implement new services.

I hope that this feedback along with an engaging dialogue today, will assist the subcommittee in continuing to move the FedRAMP program forward in a positive manner.

I thank you once again for the opportunity to share my views with this subcommittee on this important topic.