virtru

Testimony to the House Oversight and Government Reform Committee

Will Ackerly, Co-Founder and CTO, July 17, 2019

Prepared for the Government Operations Subcommittee Hearing Titled “To the Cloud! The Cloudy Role of FedRAMP in IT Modernization”

Good Morning Chairman Connolly, Ranking Member Meadows, and Members of the House Committee on Oversight and Reform, including my Representative Ms. Holmes Norton. Thank you for the opportunity to speak with you today about the Federal Risk and Authorization Management Program (FedRAMP) and our experience with FedRAMP as a technology small business.

My name is Will Ackerly, and I am the co-founder and CTO of Virtru, a Washington DC-based data privacy software company. Our mission is to empower organizations and individuals to protect their data wherever it travels. Because of this privacy mission, we take our security posture and processes very seriously, which is why FedRAMP approval was an important milestone for us, and why I am happy to be here with you today.

My brother and I started Virtru in 2012, following careers in the Federal government. He was Director of Policy and Strategic Planning at the Department of Commerce and economic advisor at White House, and I spent 8 years in the intelligence community focused on secure information sharing between intelligence agencies and mission partners. Virtru was founded on the core belief that privacy is both a fundamental right and a force multiplier for organizations. In today's digital era, protecting and controlling access to data is an essential component of privacy. Virtru's mission has always focused on making it easy for any person or organization to protect their privacy, which is why our first software release was a free application that individuals could download to encrypt and control their email. Today, we continue to deliver on this privacy mission. Virtru has expanded to over 120 employees and continues to develop privacy-enhancing software that supports individuals and organizations of all sizes to protect their data. The Virtru

Data Protection Platform is based on open data standards, leveraging the latest encryption standards, and now supports over 5000 commercial customers and multiple Federal, State & Local government customers.

We understand the importance of protecting government data and believe that programs like FedRAMP effectively improve Commercial Off-The-Shelf (COTS) security and privacy controls, enabling government agencies to focus more on achieving key mission outcomes.

Several years ago, as we considered creating new solutions beyond our consumer-focused apps, our strategy focused on building solutions for commercial markets, partly due to the high barriers of entry to work with government, such as acquisition timelines. However, in 2015 a number of government agencies, such as Veterans Affairs (VA), reached out to us to help them securely share data. As we talked to the VA and other agencies like the Federal Communication Commission and the Department of Interior, we continued to run into the question of FedRAMP. Despite being a relatively new company, working with the government to protect its sensitive data related to the health, safety, and lives of Americans was a great opportunity to make an impact. We altered our strategy, added the FedRAMP requirements to our roadmap, and began to prepare for the FedRAMP process.

Going through the FedRAMP process improved our company's overall security posture. Despite occasional challenges or confusion, of all of the compliance efforts we have gone through, FedRAMP added the most concrete security and risk management value. All of our customers now benefit from improved internal processes, and the FedRAMP effort solidified a business case for improved security.

As we worked toward FedRAMP requirements, we continued conversations with the FCC, who wanted to use our solution and were willing to sponsor us for an agency FedRAMP authorization.   We officially were in process on 6/23/2017 and received our final authorization 20 months later on 3/1/2019. For startups like us, this is a very long timeline. It was also unclear upon entering the process how long it would take, which added risk to the decision.

In retrospect, Virtru was fortunate to be able to complete the process in just under two years, and we had the advantage of being located in DC with employees who were familiar with navigating federal government processes. Long timelines and challenges relative to estimating the total length of the process pose barriers to entry for a small business with limited resources.

Cost is another challenge for small business when considering FedRAMP. Cost is always a major consideration for startups like us, and the roughly $1.6 million total cost of FedRAMP was a significant percentage of annual revenue. It had to be balanced against other financial resource allocations, such as hiring or product development. As a privacy and security company, this was a justifiable decision to make, but when combined with the unknown timeline mentioned above, it would be a high-risk decision for many small companies.

The FedRAMP process also requires significant ongoing resource requirements necessary to maintain the authorization, a point often mis-understood when first starting the process.   Even well into the process, many organizations may think FedRAMP is a one-time effort. In our experience, however the continuous monitoring requirements are a significant ongoing activity. For instance, the FedRAMP control enhancement implementations and continuous monitoring requirements are ongoing resource intensive commitments, with annual 3PAO assessments that do not cost significantly less than the original assessment.

We also found the level of support and expertise available to help successfully complete the FedRAMP process varied significantly by each government organization. This required us to adjust our implementation strategies for each specific agency lack of consistency.

As a citizen who wants the government to leverage modern IT, and as a business leader in a startup that went through the FedRAMP experience, I believe that expanding the universe of companies that are able to meet FedRAMP controls does more than protect US government data; it also improves the US public and private security posture and improves data protections for all Americans. Making FedRAMP controls more accessible and the FedRAMP process more efficient for companies of all sizes would improve our national security posture and protect private citizens and US companies against corporate espionage.

Based on our experience going through the process, I would ask the Committee to consider the following recommendations. These recommendations are not intended to lower the bar for security but rather to expedite the process, with a goal of improving security outcomes and facilitating wider adoption of FedRAMP by companies of all sizes.

- **Streamline Reassessments.** Accelerate IT modernization and innovation by ensuring the FedRAMP process allows for re-usable inheritance of controls and allowing companies to continually innovate while reducing additional costs and time for FedRAMP re-assessment. Virtru provides the best data protection capabilities we can to Federal agencies, but if we are required to dedicate resources to support FedRAMP re-assessments in order to release a new capability into the market, the ongoing costs associated with the FedRAMP process could restrict our ability to compete. There is clearly a need to be sure the new capabilities meet security requirements. However, the FedRAMP controls requirements for change management and annual third-party assessments should be presumed to be sufficient to address the associated risk.

- **Empower the FedRAMP PMO.** The FedRAMP process would be improved if the FedRAMP PMO were further empowered and resourced to educate and foster companies and agencies through the authorization and continuous monitoring processes. In order for the Federal IT environment to innovate efficiently with startups like us, FedRAMP needs to provide a way to go through one process and then be able to work across agencies. This focus on real reuse of results and evidence versus starting over at each agency would greatly improve Federal IT and allow agency IT resources to focus on other critical areas. Agencies could be further empowered by the creation of a FedRAMP lead at each agency that could both coordinate with the PMO and understand the separation of duties and responsibilities between the agency and the PMO. This person could save time through cleaner handoffs in the process and limiting the rework that gets done. Finally, this position would develop cloud security expertise and expand this expertise across agencies.

- **Empower Agency Sponsors.** Do not limit CSPs to only the Joint Authorization Board (JAB) process. The JAB can help with the increased reuse of results, but, for us, the JAB process as exists today would have made it difficult to meet specific agency mission security needs. The FedRAMP process, with its inclusion of an agency sponsor, enabled us to validate specific agency mission needs that we could meet, which allowed us to make a more informed business decision. The JAB plays an important role, but if the only option were to go through the JAB, it would have been harder to justify the expense without interest from an agency which would give us a potential roadmap to see a return on the investment. As a result, this would limit the solutions that agencies can use to manage their risk.

- **Implement a Multi-Level Authorization Structure.** Ensure any FedRAMP legislation or policy allows for appropriate risk-based decisions. It is our understanding that the JAB process prohibits connectivity or use of any non-FedRAMP approved third-party provider. This rigid, blanket prohibition significantly limits the types of services that federally focused products can leverage. At the same time, it makes it much harder for agencies to access innovative capabilities and inhibits effectively focusing on mitigating risk to Federal data. Requiring an authorized system to connect only to other authorized systems constrains functionality beyond what is needed for strong security. Using a non-authorized system to, for instance, store encrypted data should not require that the storage system have the same level of controls as a system processing unencrypted data, because of the security that travels with that encrypted data.

- **Improve transparency and enhance feedback loops.** If agencies were required to provide all of their accreditation packages to FedRAMP, not just the authorization letters, it would permit analysis of how to improve and adapt controls. Once the PMO has visibility into the accreditation packages, they could look across them to see trends such as controls that are consistently not implemented or not applicable and other common features that could be either clarified or highlighted. While NIST is the owner of Federal standards, this feedback loop could be used by both FedRAMP and NIST as they update policies and standards. With innovative Federal policy initiatives like Cloud Smart and the Federal Data Strategy that focus more on the security of the data itself versus traditional network protections, FedRAMP and NIST can work together to update controls and control baselines to reflect the needs of Federal IT and meet those policy goals. Improving transparency and expanding feedback loops related to FedRAMP packages could help confirm what is available today or show where controls and industry are misaligned.

- **Increase Timeline and Cost Transparency.** Help support innovation and increase CSPs going through the process by publishing additional data and mitigating the timeline and cost risks through increased transparency. With the PMO publicizing additional information like expected timelines with dependencies and milestones, as well as the average time it takes for different-sized companies to meet each milestone, CSPs that do not work with Federal agencies today may be able to make the business justification to enter the market. Finally, as mentioned above, highlight and clarify the ongoing required monitoring and associated costs at the outset of the process to support future planning.

- **Engage in Community Outreach.** Support a means for continued public engagement with the FedRAMP community. I am sure that many of the CSPs who have gone through or are going through the process have questions or ideas for improvement, and the government should have an easy way to leverage the combined expertise of the CSPs. Both the PMO and CSPs are incentivized to make the program successful, so there should be a way for everyone to work together.

I appreciate the opportunity to address the Committee today and look forward to working with anyone interested in the FedRAMP program or in any other way that government can improve the security and privacy of Federal data. FedRAMP was an important experience for us as a company and I believe it is an enabler for Federal IT modernization. I will gladly answer any questions you have today and am happy to make anyone at Virtru available for specific follow-up discussions.