Questions for Mr. Anil Cheriyan
Director of Technology Transformation Services (TTS)
General Services Administration (GSA)
Questions from Chairman Gerald E. Connolly

July 17, 2019, Hearing: "To the Cloud! The Cloudy Role of FedRAMP in IT Modernization"

1. What challenges exist with funding and operating the Federal Risk and Authorization Management Program Management Office (FedRAMP PMO) and the General Services Administration portion of the JAB through the Federal Citizen Services Fund? Would additional funding or a different funding mechanism enable the FedRAMP PMO and the JAB to look at and authorize more products that meet FedRAMP standards?

   Response: The continued speed and scale of agency cloud adoption, as well as the dramatic growth in cybersecurity threats, has outpaced the capacity of the program. While the FedRAMP PMO has realized internal efficiencies to increase capacity, the program is limited by resource constraints. To a certain extent, the program is scalable based on the level of resources available, therefore any additional GSA funding would allow the FedRAMP PMO and JAB (through GSA's 1/3rd cost contribution)to authorize more products. It could also be used to invest in improvements that would increase capacity for JAB and agency authorizations. This would also expand the JAB's ability to ensure the ongoing security of systems it authorizes - otherwise known as continuous monitoring.

2. In 2018, what percentage of federal agencies reused FedRAMP authorizations?

   Response: At the end of 2018, 100% of the CFO Act Agencies were reusing FedRAMP Authorizations. In total, there were roughly 125 federal organizations (agencies, sub-agencies, components, independent agencies, etc.) that were reusing products with a pre-existing FedRAMP authorization.

3. How can the FedRAMP PMO incentivize more agencies to sponsor cloud products through the FedRAMP authorization process?

   Response: The FedRAMP PMO plans continues to partner with OMB and the Federal CIO Council to explore how to incentivize agencies to sponsor authorizations and help overcome barriers that agencies face preventing the initial sponsoring of cloud products. Potential opportunity areas include: resource sharing, training, shared agency reviews, and continuous monitoring.

Questions for Mr. Anil Cheriyan
Director of Technology Transformation Services (TTS)
General Services Administration (GSA)
Questions from Ranking Member Mark Meadows

July 17, 2019, Hearing: "To the Cloud! The Cloudy Role of FedRAMP in IT Modernization"

1. What are three major obstacles that are creating delays in the authorization process, and what can be done administratively or legislatively to help address the obstacles?

Response: There are 3 major obstacles that are causing delays:

1. The current authorization process is largely manual and labor-intensive, which contributes to lengthy authorization timelines. The continued speed and scale of agency cloud adoption, as well as the dramatic growth in cybersecurity threats has outpaced the capacity of the program to keep pace.
2. There are misperceptions regarding FedRAMP's processes, and individual agency interpretations of the NIST baselines and FISMA that create reciprocity challenges. As a result, the FedRAMP PMO spends significant resources on training and outreach with individual agency representatives and Cloud Service Providers on how to accelerate the process.
3. Individual agency risk tolerances yield differing security requirements, which then causes agencies to need to work with vendors to meet their security needs, delaying the process.

We are working to address each of these areas, but opportunities still remain. Specifically, in order to address each of these areas GSA is working with all stakeholders to:

1. **Incorporate Automation:** The FedRAMP PMO is focused on exploring automation to streamline the process. FedRAMP partnered with the National Institute of Standards and Technology (NIST) beginning in May 2018 to develop the Open Security Controls Assessment Language (OSCAL), the goal of which is to automate FedRAMP's security materials into what is known as machine-readable language. This would automate many previously manual processes, increasing ease and efficiency.

   FedRAMP published its three security baselines (Low, Moderate, and High) in OSCAL format on June 1, 2019 as a key step in its overall automation efforts. This will provide a foundation to reduce time and costs, and empower future policy improvements.

2. **Engage the Community:** The FedRAMP PMO will continue its efforts to educate both agencies and industry on the FedRAMP process. In addition, the FedRAMP PMO will employ further engagement and outreach opportunities to collect feedback from all stakeholders on ways to simplify the process, clarify the documentation, and adapt the program based on evolving cyber-threats. The program will continue to work with industry to make updates to FedRAMP guidance through community insights following user-centered design best practices.

   Agency participation has increased in recent years. FedRAMP provides twenty on-demand and in-person learning opportunities for Industry and Agencies, that have been taken by approximately 12,500 individuals. As a result, agency participation in the program increased from roughly 113 agencies in (FY) 2017 to 156 today. Education and outreach will remain a top priority for the program.

3. **Develop a Threat-Based Authorization Methodology:** To better align with the dynamic nature of cyber risk and volatility, FedRAMP is partnering with multiple organizations to develop a

modular and agile approach to authorizations. Agencies will be able to use secure technology faster and industry will have a return on investment more quickly.

A threat-based approach focuses on security requirements that protect against the highest priority, known and unknown threats, according to their potential significance and consequence. For example, technical security settings and capabilities that prevent data exfiltration will be prioritized over requirements that focus on documentation-based policies and procedures.

2. Given how DOJ and HHS both operate in the national security and non-national security environments, how does this unique environment present challenges and opportunities in a FedRAMP context?

   Response: FedRAMP only applies to unclassified federal information systems - not classified or national security environments. Therefore, GSA would defer this question to DOJ and HHS for more specifics about how they leverage FedRAMP in their unique environments. Anecdotally, FedRAMP partners with national security advisors - particularly via the DOD and DHS presence on the JAB, and within the national security realm.