Statement of Anil Cheriyan

Deputy Commissioner Federal Acquisition Service and Director Technology Transformation Service, General Services Administration

Before the U.S. House of Representatives

Committee on Oversight and Reform

Subcommittee on Government Operations

July 17, 2019

Introduction

Chairman Connolly, Ranking Member Meadows, and distinguished members of the subcommittee, good morning and thank you for the opportunity to testify here today.

I am Anil Cheriyan, Deputy Commissioner of the Federal Acquisition Service (FAS) and Director of the Technology Transformation Services (also known as TTS) within the U.S. General Services Administration (GSA).

Prior to joining GSA in January of this year, I served as the Executive Vice President and Chief Information Officer at SunTrust Banks, where as part of the Executive Leadership Team, I led digital, data, and operational transformation efforts. Prior to SunTrust, I led several transformational consulting engagements as a partner at IBM and PwC Consulting.

GSA's overall mission is to deliver value and savings in real estate, acquisition, technology, and other mission-support services across government. Under that umbrella, TTS' specific mission is to improve the public's experience with the government by helping agencies build, buy and share technology that allows them to better serve the public. I firmly believe in this mission. TTS applies modern methodologies and technologies to improve the public's experience with government and helps federal agencies build, buy and share technology to achieve their digital transformation and modernization goals.

The Federal Risk and Authorization Management Program (FedRAMP) is an integral program within the TTS portfolio. FedRAMP aims to empower agencies to modernize operations using secure cloud solutions to improve agencies' information technology (IT) security. Moreover, FedRAMP is intended to streamline the authorization process.

Today, I would like to share with you some insights into FedRAMP's mission, value proposition, current landscape, and my vision of continuous improvement in the program's future.

FedRAMP’s Model and Mission

In 2011, the Office of Management and Budget (OMB) released a memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments* establishing FedRAMP to provide a cost-effective, risk-based approach for the adoption and use of cloud services to Executive departments and agencies. Per the framework established in the 2011 memo, FedRAMP consists of two key entities – the Program Management Office (PMO), which GSA operates, and the Joint Authorization Board (JAB), which consists of security experts from the Department of Homeland Security, the Department of Defense, and GSA.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. A Cloud Service Provider (CSP) can choose to pursue an agency-sponsored authorization to operate (ATO) or a provisional authorization to operate (P-ATO) issued by the JAB. - A CSP makes this determination based on its business strategy for its cloud offering. Regardless of which approach, there are three general phases that occur after a CSP decides to enter the federal market

Preparatory Phase

A CSP makes necessary technical and procedural upgrades to its product or services to meet federal security requirements. The CSP will then develop security materials to support that their product meets requirements. This assertion is verified and validated by an independent auditor, referred to as a third-party assessment organization (3PAO).

Authorization Phase

As mentioned above, there are two tracks for this phase. The first approach is when an agency conducts the security materials review; accepts the risk; and issues an ATO. This is done based on FedRAMP PMO guidelines and processes and the agency’s risk tolerance. The FedRAMP PMO receives a copy of the security materials and performs a quality assurance review to ensure that cloud offering meets FedRAMP requirements. Then, the FedRAMP PMO includes the offering in the FedRAMP Marketplace and makes it available for reuse by other agencies. The FedRAMP Marketplace lists all authorizations available for government-wide reuse. The agency authorization approach accounts for roughly 75% of FedRAMP authorizations issued. Under this track, the agency is responsible for continuous monitoring not the JAB. Specifically, CSPs are required to deliver periodic reports to all agency customers to ensure federal information continues to be protected throughout the government’s use of the product.

The second track is when a CSP’s security materials are formally reviewed by the JAB. All three JAB agencies review security materials and issue a P-ATO. A major factor in determining whether the JAB will review a product is based on federal demand. FISMA requires agency heads to be responsible for information security risk within that agency and, while FedRAMP attempts to help streamline and support agency risk determinations, ultimately that responsibility lies with the individual agency. This approach accounts for the remaining 25% of FedRAMP authorizations. In addition, to the review, the JAB and FedRAMP PMO will perform continuous monitoring for products with a P-ATO. Specifically, CSPs are required to provide periodic security reports to the JAB and FedRAMP PMO. Then, the FedRAMP PMO reports out monthly to the agency community on the cloud offering's security posture.

Reuse
Reuse occurs when an agency accepts a JAB provisional authorization or another agency's authorization. According to FISMA, this still requires the new agency to conduct its own risk assessment. Under FedRAMP, the additional authorizations are streamlined based on the prior work of the JAB or the initial sponsoring agency.

While each path follows different steps, the same FedRAMP processes and checks are built into both paths to ensure the creation of a unified security standard for all cloud products and services and allow for ATOs to be reused. As a result, the government's security posture is improved; authorization costs are lowered for both government and industry, and authorization efforts among agencies are streamlined. On the macro scale, FedRAMP has resulted in significantly greater cloud adoption across the federal landscape.

The FedRAMP Landscape

I would like to take this opportunity to walk through the progress FedRAMP has made in recent years and highlight some key trends.

First, the pace of FedRAMP Authorizations has grown significantly and will continue to do so. In fiscal year (FY) 2018, the government issued approximately 40 FedRAMP Authorizations, inclusice of both P-ATOs and ATOs. By comparison, it took three years to authorize the program's first 40 cloud products. Today, we have a total of 143 cloud products from 115 companies that have achieved a FedRAMP Authorization and another 69 cloud offerings are in the JAB and agencies' pipelines to achieve authorization. We expect the number of FedRAMP authorized products to continue to grow at a fast pace for years to come.

Importantly, the number of authorizations being reused is also growing. When factoring in the current average reuse of approximately 8 times per authorization, the 143 cloud products we have today result in roughly 1,141 authorization reuses that can be used with an estimated $285 million in cost avoidance for the federal government as well as the time and effort saved by CSPs.

Second, authorization timelines have decreased. FedRAMP developed and implemented several improvement efforts to reduce authorization timelines. In FY2018, the average JAB authorization timeline was reduced to approximately 5.5 months; a decrease compared to over 13 months in FY2015. Agency authorization timelines have also decreased in FY2018, averaging approximately 8 months compared to roughly 15 months in FY 2015.

Third, agency participation has increased in recent years. The FedRAMP PMO encourages agency participation through training and reinforcing the 'do once, use many times' reuse approach. 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.

Areas for Improvement

However, despite maturation of the FedRAMP process, the PMO has identified several opportunities for continued improvement:

- A lack of understanding of the FedRAMP process (including how it relates to the full life cycle for the procurement and authorization of a CSP at any particular agency), and the associated roles and responsibilities of CSPs and agencies, can result in misperceptions on the timelines and cost of an authorization; e.g., the preparation time CSPs need to address underlying technical issues; or the time to develop or review the security materials required for an authorization. These misperceptions can potentially dissuade a CSP from undertaking the FedRAMP process or an agency from participating in the process.
- While FedRAMP has made efforts to assist industry through intake meetings, communication with industry can be strengthened. There is no central forum for agencies and industry to share information in a data-driven manner, and as a result, there are several anecdotal stories of FedRAMP that persist for multiple years - perpetuating outdated perceptions or worse, still leaving real issues unaddressed. Ultimately, better transparency and clear understandings of roles and responsibilities – from agencies, from the FedRAMP PMO and the JAB, and from industry providers can help to ameliorate some of the confusion around the authorization process and provide better results for all parties involved.
- Most significantly, the process still takes a significant amount of time.

To that end, the FedRAMP team is working on several new efforts to increase authorization speed and implement process efficiencies to boost agency acceptance and reciprocity of FedRAMP Authorizations:

- **Incorporating automation in the authorization process**

  FedRAMP partnered with the National Institute of Standards and Technology (NIST) to develop the Open Security Controls Assessment Language (OSCAL) to automate FedRAMP's security materials into machine readable language. This will provide the vendor and agency community the ability to reduce time and costs associated with manual, labor-intensive processes that exist today.

- **Threat-based authorization methodology**

  To better align with real-world cyber risk and volatility, FedRAMP is developing a modular, agile approach to authorizations so agencies can use secure technology faster and industry realizes return on investment more quickly. With this approach, agencies will make risk-based decisions by focusing on security controls that protect against known and potential significant/consequential threats.

- **Formal feedback mechanisms**

  The American Council for Technology and Industry Advisory Council (ACT /IAC) is creating a formal FedRAMP working group with participation from agencies and industry. FedRAMP will participate in this and other industry / agency joint working groups to exchange information and data on topics relating to the cloud authorization process.

Conclusion

In conclusion, I'd like to summarize my statement in a few words:

- I believe that FedRAMP's mission to empower agencies to modernize its infrastructure using secure cloud platforms in the most rapid, scalable, and effective method is integral to TTS and GSA's broader mission.

- I believe that FedRAMP's "do once, use many times" foundational principle reduces costs and saves time for both industry and government, and we will actively work with agencies, OMB and Congress to find ways to increase reciprocity.

- I am committed to leveraging my role and industry experience to work closely with all our partners to make FedRAMP as open, efficient, and secure as possible.

- Finally, I welcome further feedback and engagement with the Committee to evaluate additional improvement opportunities.

Again, thank you and I look forward to the opportunity to answer your questions.