TESTIMONY OF

Jose Arrieta

Chief Information Officer

U.S. Department of Health and Human Services

Before the

Subcommittee on Government Operations

Committee on Oversight and Government Reform

U.S. House of Representatives

July 17, 2019

Good morning Chairman Connolly, Ranking Member Meadows, and Members of the Committee. Thank you for providing me the opportunity to discuss the Department of Health and Human Services' (HHS) participation in the Federal Risk and Authorization Management Program (FedRAMP). I appreciate the opportunity to speak with the subcommittee today to share my perspectives on this program; a program that has enabled departments and agencies across the Federal government to more effectively secure and adopt cloud technologies, increase cost savings, and decrease dependencies on legacy information technology and infrastructure. I was appointed as the HHS Chief Information Officer (CIO) on May 28, 2019. And, as the HHS CIO, I am keenly aware of the value and importance of leveraging cloud technology to drive greater data sharing, greater data security and greater financial savings.

HHS and the FedRAMP Program

Beginning in 2013, HHS has embraced both emerging cloud technologies and the FedRAMP process becoming the first agency to sponsor a cloud service provider through the FedRAMP process. These initial efforts resulted in cybersecurity authorizations for two cloud-based infrastructures and allowed other Federal departments and agencies to leverage those services as well. Since that time, the Department has endeavored to be on the cutting edge of cloud security and FedRAMP. In the past five years, the Department issued the initial authorization for 14 cloud service providers and currently maintains authorizations for nine unique cloud offerings.

Across HHS, over 60 FedRAMP certified cloud technologies and services are in use, including those sponsored by HHS. HHS also ensures that program-specific, mission critical, products are sponsored where possible. Due to the unique nature of HHS' mission, which is to enhance and protect the health and well-being of all Americans, commercial off the shelf software may not meet the high security bar the Department requires based on the populations we serve and the information we protect. This is why the FedRAMP program is critical to the Department. By having a Federal-wide cloud security standard, agencies are able to effectively determine the security and risk associated with each service. This 'do once, use many' model has saved the Department and its customers countless hours of security assessment time by being able to review and utilize existing documents that have already been approved by other agencies. HHS uses over 60 FedRAMP authorized cloud products which were initially reviewed by other agencies and sponsors. To further this methodology, HHS has worked with other agencies to conduct security assessments and share resources.

FedRAMP Best Practices in HHS

HHS adopts and leverages FedRAMP processes and sponsors cloud providers for three reasons.

First, HHS screens the cloud technologies to ensure that they support the HHS mission. The cloud technology typically enables research across large data-sets, streamlines processes by decreasing both processing times and cost, and ensures scalability of the HHS systems.
Second, our efforts with cloud technologies help ensure that HHS maintains and manages its risk posture. The HHS cloud security and FedRAMP Program ensures that cloud service providers deployed across HHS are properly and appropriately authorized based on HHS' risk posture and risk tolerance. It provides Federal-level cloud security leadership and visibility, in addition to providing resources to accomplish HHS' mission and goals at significant cost savings.

Third, HHS sponsors cloud providers because the FedRAMP process ensures that the work we do at HHS can easily be leveraged and reused by other departments and agencies across the Federal government. This is one of the ways that HHS supports shared services across the Federal community. HHS also believes that cloud adoption is vital for information technology to thrive; our efforts help bring more cloud services and technologies to that ecosystem.

We remain engaged with both the FedRAMP process and the program management office established by the General Services Administration to ensure that our processes are tightly aligned and continue to evolve while learning from the experience of others. Internal to HHS, we've facilitated a number of events promoting the FedRAMP process, including an agency-wide FedRAMP Day and workshop and panel participation at HHS information technology events and gatherings. More broadly, the HHS cloud security team has participated in numerous GSA FedRAMP sponsored panels and events on a wide variety of topics, such as continuous cybersecurity monitoring, FedRAMP best practices, and general FedRAMP process training.

Identification of Risk in Cloud-Based Systems

The key purpose of the FedRAMP program is to ensure that risks associated with cloud services are surfaced and their potential impacts are clearly understood and appropriately mitigated. Cybersecurity risks exist in every system; at no time will any information technology system, whether it's based in legacy data center or the cloud, be free of risk. It is critical, therefore, that Federal consumers of cloud technologies and services – departments and agencies – understand the cybersecurity risks associated with a specific cloud technology. HHS is responsible for protecting the data of one in three Americans; that data sometimes includes personally identifiable information (PII) and protected health information (PHI), both deserving of comprehensive protection. Having a clear understanding of the risk associated with using a particular cloud technology – given the information HHS is charged to protect – is critical. The FedRAMP program enables this.

The FedRAMP authorization process is comprehensive and consistent with the cybersecurity requirements laid out in guiding Federal legislation such as the Federal Information Security Modernization Act of 2014. An average cloud system requires in-depth documentation and testing of over 300 separate security controls – technical controls that govern things like access to the system, how and when information is backed up, and how computer log files are reviewed. At the end of this sometimes arduous process is a complete and comprehensive picture of the cybersecurity risks departments and agencies must accept and monitor in order to use that cloud technology.

The FedRAMP process at HHS isn’t just about a point-in-time authorization of a specific technology. The process enables a constant understanding of risk and how that risk changes over time. Leveraging the model established by the FedRAMP PMO, HHS uses a continuous monitoring approach to ensure that cloud technologies and systems maintain an acceptable level of risk. We meet with cloud service providers’ technical and security staff on a monthly basis to review results of regular security scans and tests to gauge progress against the remediation of cybersecurity issues or weaknesses. We conduct an annual review of each cloud service provider we sponsor. This review represents a comprehensive assessment of a subset of critical security controls through the use of vetted third-party testers. Finally, for those cloud service providers who fail to adequately maintain and remediate risk, we have an escalation process that we leverage to ensure that risks are appropriately remediated within fixed periods of time or else the HHS authorization is revoked. This continuous monitoring approach ensures that we manage risk over time instead of relying on a single point-in-time assessment.

Reuse of FedRAMP Documentation and Authorizations

As previously noted, the process to authorize systems for use within the Federal government is necessarily comprehensive. Ensuring that cloud-based technologies and systems meet all Federal cybersecurity standards takes time. The process requires a great deal of documentation to ensure that consumers of the system have the ability to fully understand how cybersecurity controls are implemented to protect government data. Each of these security controls must be thoroughly tested and the results of these tests – the risks associated with system use – must be clearly documented and presented.

The FedRAMP process promotes reuse, recognizing that, once a FedRAMP authorization exists for a cloud provider, a significant investment of time and resources has already been committed to a specific cloud system or technology. The process ensures that the cybersecurity authorization activities conducted in one part of the government are able to be leveraged by another without the need for duplicative authorization process. Regardless of where a FedRAMP authorization is conducted – HHS, another agency or through Joint Authorization Board– other Federal consumers should be assured that an appropriate level of rigorous risk assessment and risk management has been applied to a system. This should alleviate the need for that comprehensive process to be repeated elsewhere, which creates cost-saving efficiencies to better steward taxpayer dollars.

Successes of the HHS FedRAMP Program

Many cloud providers that HHS sponsors have realized a large number of secondary benefits after obtaining their initial FedRAMP authorization, including the ability to provide services to state and local entities. While FedRAMP was initially conceived as a Federal standard, our Department identified a number of state agencies that prefer the use of FedRAMP authorized products, as their respective states do not currently have a cloud security standard.

Additionally, vendors have reported that many of their commercial customers request a FedRAMP compliant version of their products due to the higher level of rigor focused on cybersecurity and risk management. The security teams at these vendors have also commended FedRAMP as it has prompted their business to improve the overall security of their other products and third-party companies.

The HHS FedRAMP team is regularly recognized internally and externally for its expertise, exceptional training and customer support. Over the past year, the team has been the recipient of three awards:

- 2018 FedRAMP Five Winner, Large Agency Category
- 2018 FedRAMP Five Winner, Future Leader
- HHS Office of the Chief Information Officer’s (OCIO) 2018 Third Quarter Innovation Award Winner

FedRAMP and Cloud Challenges

Cloud use and the FedRAMP process has been exceptionally beneficial to HHS by expanding the market of cloud services and technologies open to us, and also provides opportunities for improvement. Sponsoring cloud services and technologies through the FedRAMP process requires resources, expertise and commitment at a time when many agencies are resource-constrained. Cloud sponsorship competes with the myriad other cybersecurity requirements and initiatives requiring daily attention across the Federal sector. While HHS has been able to identify and retain the resources necessary to sponsor cloud technologies, many agencies may face challenges since there is a consistent demand for new cloud-based services which, prior to use, must be authorized using FedRAMP processes.

While sponsorship requires the government’s time and attention, the vast majority of work falls to the cloud service provider. The provider must leverage the FedRAMP processes and templates to ensure all documentation is completed with the appropriate level of detail, and that system is tested to ensure the cybersecurity controls operate as described. While large corporations likely have both the talent and financial resources to address FedRAMP requirements, smaller businesses and organizations may not. This may result in the government's inability to obtain the highly-specialized cloud-based capabilities it needs. We expect that the recently released FedRAMP tailored process will alleviate some of these concerns.

Another key challenge HHS has observed focuses on cloud service providers' ability and commitment to maintain an appropriate level of risk mitigation after a FedRAMP authorization is issued. Maintaining the cybersecurity posture of large, cloud-based environments is a significant undertaking and a cloud service provider's responsibilities do notend when their FedRAMP authorization is issued. They must monitor and collaborate with the government continuously to ensure that government customers have a consistent understanding of the system's risk posture. This requires the commitment and resources to continuously assess, report and maintain risk. Cloud service providers must – but sometimes do not – understand this prior to FedRAMP sponsorship and authorization.

Currently, there are few penalties for non-compliance if a cloud provider fails to follow FedRAMP requirements after being sponsored through the process. HHS has developed its own process to handle these issues but we would encourage standardized, government-wide process for FedRAMP oversight and enforcement in such situations.

HHS has expended a great deal of effort educating its community about FedRAMP processes and requirements but there still exists a lack of awareness in some pockets of the Federal community. Ensuring the entire Federal community – other Federal agencies, - industry partners and cloud service providers, and the Joint Authorization Board - understands FedRAMP processes and requirements is critical. We must also ensure that the Federal community evolves FedRAMP processes and requirements with the pace of emerging technologies and risk-management best practices. HHS is committed to doing so.

In Closing

HHS has experienced great success with the adoption of cloud services, technologies, and capabilities leveraging the FedRAMP program. It provides the government with a consistent and repeatable model for assessing and understanding the risks associated with cloud-based products, and reduces overall level of effort by promoting reuse of FedRAMP documentation.

Since its inception, the FedRAMP Project Management Office (PMO) has been a strong partner to HHS and has always been willing to assist the Department with any issues. While the challenges noted previously exist, the benefits realized through the adoption and migration to the cloud outweigh the challenges we have observed. We look forward to continued success and partnership under the FedRAMP program. It is clear that future software innovation will occur in the cloud, and HHS is excited to harness these new tools. HHS is committed maintaining its leadership position in government by being an early and responsible adopter of FedRAMP products and ensuring that security remains a primary focus. I appreciate the opportunity to serve as HHS CIO and support the Department’s mission through technical innovation.