STATEMENT BY

JOHN W. WILMER

DEPUTY CHIEF INFORMATION OFFICER FOR CYBERECURITY

DEPARTMENT OF DEFENSE

BEFORE THE

HOUSE OVERSIGHT AND REFORM COMMITTEE

SUBCOMMITTEE GOVERNMENT OPERATIONS

ON

“FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM"

JULY 17, 2019

NOT FOR PUBLICATION UNTIL

RELEASED BY THE HOUSE OVERSIGHT AND REFORM COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the effectiveness of the Federal Risk and Authorization Management Program (FEDRAMP) for the Department of Defense. I am Jack Wilmer, the Deputy Chief Information Officer for Cybersecurity and the Chief Information Security Officer for the Department of Defense. I am responsible for DoD cybersecurity policy, I provide technical and program oversight, and I lead engagements with the interagency and industry on matters related to DoD cybersecurity. I also serve by delegation from the DoD CIO as one of three chairs of the FedRAMP Joint Authorization Board (JAB).

Today, I will provide background on DoD's participation in FedRAMP, the effectiveness of FedRAMP, and the synergy between DoD and the FedRAMP PMO to provide authorization for cloud services for the Federal Government.

DoD Support to FedRAMP

DoD has been a part of FedRAMP since its inception, and our involvement has been a major benefit to the Department. We have leveraged FedRAMP to make 145 cloud service offerings available for use in DoD.

DoD support to FedRAMP is primarily provided by two organizations. My office within DoD CIO provides strategic programmatic support and oversight through the JAB, and also serves as the DoD Technical Review authority for the FedRAMP Program Office. We also leverage the Defense Information Systems Agency (DISA) to provide technical assessments and continuous monitoring support to FedRAMP.

FedRAMP JAB and Cloud Service Authorizations

The FedRAMP JAB is a critical collaboration venue for improving Cloud cybersecurity practices across the Federal Government. It is the approver of the published cloud cybersecurity requirements, setting the standards the providers/offerings need to meet, and that the Third Party Assessment Organizations (3PAOs) use to assess compliance. The JAB also provides the strategic direction for FedRAMP, and promotes efficiency in cloud cybersecurity authorization practices that transcend many of the interagency boundaries in the Federal Government through the issuance of JAB Provisional Authorization to Operate (P-ATO) to cloud service providers.

A JAB P-ATO allows the Federal Government to evaluate cloud service offerings once, and re-use many times. Federal Mission Program/System Owners leverage the risk information enumerated by the JAB in the P-ATO. As of June 1, 2019, there have been 722 reuses of JAB authorized services resulting in $180.5M in cost avoidance across the Federal government.

With the extensive list of cloud service offerings that exist across industry, the JAB is not resourced to assess all of the various offerings, and as such, we have to prioritize which services the JAB will assess. Our prioritization factors are published on the FedRAMP website, and include factors such as demand, and whether or not the cloud service provider is currently capable of meeting FedRAMP security standards. Once the JAB has authorized a cloud service provider, we also perform continuous monitoring of the cloud service offerings, which provides assurance to Federal Agencies that the providers maintain their security posture.

To support use of cloud service offerings which are not yet prioritized to obtain a JAB P-ATO, federal agencies can also perform their own agency assessment of a cloud offering. Following their assessment, they can issue their own Authority to Operate (ATO), or in the case of DoD, issue a Provisional Authorization (PA). The agency can then make their assessment and authorization information available to the greater federal community to leverage in subsequent authorization decisions.

Regardless of whether a cloud service offering has a JAB P-ATO or an agency authorization, the mission owning Authorizing Official (AO) retains the responsibility for making the risk-based decision for use of all systems and data upon which the mission is reliant, and ultimately make the decision to issue an ATO for the system/data residing in the cloud.

DoD Specific Requirements

DoD has greatly benefited from its partnership with FedRAMP, however, we are also required to meet Committee for National Security Systems (CNSS) cybersecurity requirements for National Security Systems. FedRAMP's processes and practices are used as the foundation for the DoD Provisional Authorization (PA) process, and account for the vast majority of CNSS cybersecurity requirements. The FedRAMP moderate baseline consists of 325 security controls, and DoD adds up to 38 additional controls to meet the unclassified CNSS cybersecurity requirements for Controlled Unclassified Information (CUI). In addition, DoD does consider cloud service providers who process CUI to be a part of our network, so we also assess their ability to perform DoD specific functions, such as procedures for dealing with spillages of classified information. Our PA process is integrated into the overall FedRAMP process, and requires on average 6 weeks depending on the complexity and sensitivity of the system.

To date, DoD has issued 130 PAs through FedRAMP reciprocity without any additional DoD evaluation. We have also granted an additional 20 PAs by assessing the extra DoD controls on top of the FedRAMP authorizations. DoD has only issued 5 PAs that were started essentially from the first control.

FedRAMP Improvements

FedRAMP's processes have evolved significantly since its inception. In FY2018, the average JAB authorization timeline was reduced to approximately 5.5 months; a decrease compared to the FY2015 average of more than 13 months. The process was modified to ensure that Cloud Service Providers were ready prior to entering the FedRAMP process, assessors understood the scope of the controls required for review, and validators understood the architecture of the offering. This triad of preparation and understanding establishes a strong path for successful completion of FedRAMP activities. Additionally, minor changes to a cloud offering such as new services or features have a streamlined path to authorization which can occur in 4-6 weeks.

DoD Process Improvements

As the Department continues its transition to the cloud, it is becoming more important to increase the speed of authorizing new cloud capabilities. One change we are making in this regard is that a universal PA will be issued for storing and processing of DoD public information on any cloud service offerings which are assessed at the FedRAMP moderate baseline. Previously, individual PAs were granted for each service offering, and this change will allow better utilization of resources for continuous monitoring and new authorizations.

DoD also continues to review opportunities to improve authorization timelines through communication with vendors and interagency stakeholders. We regularly review our control baselines with the FedRAMP PMO, with the intent of driving as much as possible consistency across the Federal Government.

Conclusion

I want to emphasize the importance of FedRAMP and the standardized approach the program provides for cloud products and services. This approach saves money, time, and staff required to conduct the Department's security assessments. Thank you for the opportunity to testify this afternoon, and I look forward to your questions.