Department of Justice

STATEMENT OF

JOSEPH F. KLIMAVICZ
DEPUTY ASSISTANT ATTORNEY GENERAL AND
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"TO THE CLOUD! THE CLOUDY ROLE OF FEDRAMP IN IT MODERNIZATION"

PRESENTED

JULY 17, 2019

Statement of Joseph Klimavicz
Deputy Assistant Attorney General and Chief Information Officer
U.S. Department of Justice

Before the House Committee on Oversight and Reform,
Subcommittee on Government Operations

At a Hearing Entitled, “To the Cloud! The Cloudy Role of FedRAMP in IT Modernization”

Presented on
July 17, 2019

Good morning Chairman Connolly, Ranking Member Meadows, and distinguished members of the Subcommittee.

Thank you for your continued commitment to improving information technology across the federal government, and thank you for the opportunity to appear before you today as the Department of Justice Chief Information Officer. This testimony provides an overview of the Department’s use of the Federal Risk and Authorization Management Program (FedRAMP), some areas for improvement, and considerations for the federal government and its partners as we begin shaping the next iteration of FedRAMP.

Under my leadership, the Department of Justice is delivering large-scale and complex IT transformations through shared services to meet the priorities laid out in the President’s Management Agenda. The following are examples of our efforts:

The Department is finalizing the migration of numerous disparate legacy email systems from on-premise facilities to a single commercial cloud provider. To date, we have moved 41 out of 43 components. Consolidation of infrastructure and licenses into a single Department-wide offering not only reduces cost, but also enhances collaboration among component agencies, simplifies operations, and improves security management.

In 2014, we began our data center transformation initiative. The Department has reduced the number of data centers from 110 to 15; we plan to close 12 more by the end of 2020. The majority of our workloads moved to commercial cloud environments, substantially increasing system resiliency, enhancing security, and optimizing operational efficiencies.

Since 2007, the Department has operated a cybersecurity shared service supporting 23 federal agencies. We recently expanded our offerings to include security operations and an enhanced trusted internet connection to optimize cloud traffic. This connection supports dedicated cloud traffic speeds up to 50 times faster than accessing the Internet from within the Department. Offering these services to agencies enhances information sharing across the government and strengthens overall federal resilience to cyber threats.

To facilitate networking and telecommunications modernization, the Department was one of the first agencies to release a solicitation under the General Services Administration (GSA) Enterprise Infrastructure Solutions contract, a government-wide $50 billion, 15-year contract. The Department is projected to spend about $1 billion over the life of the contract to aggregate buying power, drive down costs, improve service capabilities, and reduce the number of disparate contracts.

The Department has embraced commercial cloud for our critical mission applications. We have aggressively pursued developing case management systems natively in the cloud, which enables code-sharing and cost avoidance for the Department. The Department has developed and implemented the Capture program at the United States Marshals Service to replace multiple end-of-life case management systems for custody management, prisoner transport, and fugitive management. At the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Department is implementing the Spartan program to replace a set of investigative and industry inspection case management systems with an integrated suite of applications.

The Department also implemented a robust acquisition review process to oversee IT investments across the entire organization, enabling us to achieve major transformation successes. This process allows us to avoid unnecessary acquisitions and to consolidate buying power to achieve cost savings and economies of scale. Most importantly, we can aggressively pursue the shared service model of "build once, use many times" across a large and federated Department.

FedRAMP and the Department of Justice

All information systems which process, store, or transmit federal data must implement security controls as prescribed by the Federal Information Security Management Act (FISMA), requiring an independent assessment of security controls to obtain an Authorization to Operate (ATO).

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based products and services. The FedRAMP Program Management Office (PMO) established the Joint Authorization Board (JAB), comprised of representatives from the Department of Homeland Security (DHS), Department of Defense, and GSA, to serve as the authorizing entity and issue Provisional-ATOs. A Provisional-ATO means that the JAB has reviewed and approved the cloud service's system security implementation, as certified by an independent Third Party Assessment Organization (3PAO), for federal agencies to leverage when authorizing cloud services.

The FedRAMP process allows the Department to efficiently implement cloud solutions in a secure manner. To date, the Department of Justice takes advantage of 18 JAB-authorized Provisional-ATOs and nine ATOs sponsored by other agencies. The Department is the sponsor of nine ATOs which can be used by other agencies.

Additionally, the Department incorporates FedRAMP requirements into acquisition policy and contract language. Awarding contracts with this language holds vendors accountable for the implementation of security controls.

Opportunities to Improve FedRAMP

Like any government program, opportunities exist to improve throughput, automation, and standardization.

One of FedRAMP's goals is to promote the re-use of Provisional-ATOs to reduce administrative and cost burdens for both Cloud Service Providers and federal agencies. Many Cloud Service Providers, especially those unfamiliar with federal cyber requirements, do not know which security controls to prioritize and implement. Also, the predominantly manual 3PAO assessment process results in less standardized outputs and lengthened review times.

The cloud has opened new methods for small companies to develop disruptive technologies at lower cost. Opportunities exist to support their understanding and implementation of security requirements in a more automated and cost-effective manner.

Agency-level ATOs can be difficult to share because residual risk from tailored or risk-accepted controls are inherently different between entities. Furthermore, the residual risks are not consistently documented.

FedRAMP also fails to address all federal security mandates. For instance, personnel security does not extend to requiring U.S. Citizenship, data residency is not limited to United States territories, and Continuous Diagnostic Monitoring (CDM) capabilities are inconsistently implemented.

Finally, FedRAMP authorizations do not eliminate all Agency assessment, authorization, and monitoring activities. Agencies must still assess controls not implemented by Cloud Service Providers as well as provide for the FISMA-required continuous monitoring of these same cloud-based IT systems for the entirety of its operational lifecycle.

Considerations for the Next Iteration of FedRAMP

As the federal government and its partners shape the next iteration of FedRAMP, I am glad to offer a few observations for improvement.

First, an automated security assessment methodology could be developed to allow third parties to assess Cloud Service Providers in real-time. This would produce a cybersecurity risk score for Provisional-ATOs, reducing the cost and time investment of service providers.

Second, replacing manual 3PAO reviews with a real-time assessment of platforms based on technical measures – machine output only – and issuing Provisional-ATOs based on risk scores will eliminate the long wait times for manual reviews by the FedRAMP PMO.

Third, require Cloud Service Providers to use and conform to DHS's CDM standards for continuous monitoring to increase threat awareness and enable consistent cyber reporting.

Fourth, require an independent federal entity (e.g., the Federal Chief Information Officers Council or Federal Chief Information Security Officers Council) to review JAB Provisional-ATOs to ensure standards are consistent with federal policy updates.

Fifth, establish standardized acquisition clauses through the Federal Acquisition Regulatory Council to capture federal government policies and mandates (e.g., DHS Binding Operation Directives, Supply Chain requirements through various appropriations).

Conclusion

As you can see, FedRAMP is a critical part of implementing the Department's IT modernization efforts. The Department looks forward to working with this Subcommittee, the FedRAMP PMO, and the Office of Management and Budget on the next iteration of FedRAMP. Thank you again for the opportunity to appear before you today. I welcome your questions.