



Secure solutions at speed

FedRAMP-authorized cloud services can dramatically accelerate IT modernization efforts.

Recognizing the signs and addressing the challenges of aging technology have never been more important. “We’re in the epicenter of a situation with an imperative to modernize legacy technologies—and with a heightened sense of urgency,” said Raj Parameswaran, president, information technology, Maximus Federal.

The impact of aging technology on mission achievement was felt more profoundly with the workforce shifts necessitated by COVID-19. “Government stakeholders are feverishly working to modernize, [but] obsolete technology is hindering service delivery and posing security threats and data privacy issues,” he said. Maximus Federal’s focus is enabling service delivery aligned to agency business mission by leveraging applied technology and innovation.

Parameswaran said he views the drivers of technology modernization in three broad categories: mission, financial, and constituents. “A convergence of factors presents a compelling need,” he said. “The theme across government is to deliver service to constituents. In today’s environment, expectations are much higher. This is a unique opportunity.”

For agencies seeking a more-strategic approach to IT modernization, Parameswaran recommended a cloud-based platform with FedRAMP authorization. “The platform provides for business agility. The cloud solutions and services provide for innovation. The FedRAMP security framework provides for security posture,” he said.

With the variety of cloud services available, the key to smart modernization is identifying the best solution set for the consumer’s needs, and ensuring requisite security strength is a major factor.

“There is a slew of proven services and platforms in the market today, nearly 200

“In today’s environment, expectations are much higher. This is a unique opportunity.”

– RAJ PARAMESWARAN, PRESIDENT, INFORMATION TECHNOLOGY, MAXIMUS FEDERAL

with FedRAMP authorization,” he said. Among those that best align with agency security posture and risk requirements, a significant number are software-as-a-service offerings, he said. SaaS allows agencies to leverage the comprehensive and complete security framework that addresses all of the controls, at both the infrastructure and platform layers, that support the software application itself.

“If you are looking for a specific type of functionality to support a mission,” he advised, first FedRAMP-authorized SaaS solutions before approaching the need from a traditional model set.

Parameswaran described a recent experience in which the Maximus team designed and deployed a solution to support a COVID-related requirement—without knowing future scale. The need was a service delivery platform designed to support assimilation and dissemination of time-sensitive information, a robust platform to establish communication channels, receive and securely store sensitive data, and deliver information back to constituents and citizens.

The time frame: less than a week to stand up the entire operation. “I could not have imagined doing this a decade back. I don’t think it would have necessarily been possible,” he said. The solution relied heavily on FedRAMP-authorized cloud technology.

“We were able to architect a solution using a configuration that met the program requirements from a business

standpoint and that also provided for the desired security posture,” and within agency timeframes, he said. The traditional model would have had a much longer time-to-delivery, with procurement, infrastructure build-up, application development, and a lengthier ATO process, he added.

Cloud adoption offers a mechanism for achieving technology modernization goals, he said, and FedRAMP helps drive and stimulate cloud adoption. Leveraging these in tandem provides a strategic opportunity for government agencies to transform their IT environments, to “successfully pivot to delivering efficiently on mission programs—and some of these mission objectives have changed,” he said.

From a scope and functionality standpoint, cloud services also are evolving. “It used to be infrastructure-as-a-service and platform-as-a-service. Now there are [SaaS] models ... that have evolved to more hybrid and integrated applications: the concept of ‘everything as a service,’” he said.

Parameswaran described another situation, one that was echoed across organizations: when COVID-19 necessitated the rapid pivot to telework, Maximus was faced with ensuring employee health was safeguarded while continuing to deliver government services securely. “We had a well architected design for VPN and VDI, but it was clearly not designed for the entire workforce to be working remotely in a matter of one week,” he said.

Maximus leveraged services scaled on demand to enable its own workforce, and FedRAMP authorization allowed streamlining services for continuity. “Having expertise in cloud space and supporting several federal agencies with FedRAMP authorized solutions has been a plus,” he said.

SPONSORED BY :