Consistent Federal IT Rules May Ease State and Local Cloud Adoption

Justine Brown | February 17, 2012

It may not be long before the federal government becomes a power user of cloud computing, potentially diffusing its reputation as a slow adopter of cutting-edge technologies.

The Federal Risk and Authorization Management Program (FedRAMP) is just a part of the 25-point plan for federal IT reform announced by former Federal CIO Vivek Kundra in December 2010. Among other things, that plan set deadlines for federal agencies to adopt " cloud-first" strategies. And while federal budget cuts, a looming presidential election and a change in CIOs have raised some question as to FedRAMP's future, new Federal CIO Steven VanRoekel is committed.

On Dec. 8, 2011, VanRoekel, along with the U.S. General Services Administration (GSA) Associate Administrator David McClure, Department of Homeland Security (DHS) CIO Richard Spires, and National Institute of Standards and Technology's Director for the Information Technology Laboratory Charles Romine, held a conference call with reporters formally announcing FedRAMP, thereby solidifying the fed's commitment to the program.

“Cloud computing offers a unique opportunity for the federal government to take advantage of cutting-edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens,” VanRoekel said during the call.

VanRoekel added that FedRAMP would go live within the next year — a move projected to save the government 30 to 40 percent on cloud computing costs.

What is FedRAMP?

FedRAMP is an interagency initiative being led by the GSA. The program’s goal is to develop a governmentwide certification process to reduce costs and duplication when multiple agencies attempt to certify products and services for security compliance. Under FedRAMP, a cloud computing provider’s services can be authorized just once, and other agencies can piggyback on that authorization, instead of conducting individual accreditation.

“FedRAMP will reduce duplicative efforts, costs and inconsistencies we currently face with the security authorization process,” said McClure.

Security controls around cloud computing are a high priority because while the Obama administration has advocated the adoption of cloud computing by federal agencies as a means to reduce costs, IT experts have consistently pointed to lack of security and the lack of a governmentwide authorization program as the biggest barriers to adoption. Spires has experienced this at his agency. “ On the public side, we are doing things at DHS with some of our public-facing data, but we have been reluctant to use cloud,” he said. “The big concern has always been making sure we have that security clearance. For that reason, we have not yet aggressively pursued a public cloud capability.”

McClure agrees. “The security issues have been the key impediment of the federal government using cloud capabilities,” he said. “ FedRAMP changes that by mapping out the baseline required security controls for cloud systems, and thus creating a consistent set of security guidelines for cloud computing.”

Federal adoption of cloud computing is inevitable, says Jennifer Kerber, vice president of federal and homeland security policy for TechAmerica, an industry group which has advocated for streamlining the accreditation process for cloud vendors. “The only question is if it will be done in a secure or insecure fashion. The FedRAMP program could be the game-changer in this equation.”

Making Progress

McClure said VanRoekel’s December announcement gave the FedRAMP Joint Authorization Board (JAB) — led by the GSA, DHS and Department of Defense — approximately 180 days to become operational. “We are currently in a prelaunch set of activities, making sure all the security controls are in place,” he said. “On or around the 180th day, we’ll move into initial operating capacity with an initial set of cloud services being offered through FedRAMP.”

JAB’s role is to evaluate and approve accreditation criteria for independent third-party organizations that’ll provide assessments of cloud service providers’ compliance with

FedRAMP. Those third-party assessment organizations will be rigorously evaluated and tested to ensure they have the appropriate skills to perform such assessments. The approved assessors will charge cloud services providers to analyze their software or hardware to ensure it meets the FedRAMP standards. Working with the cloud provider, an assessor will gather data and then report its security evaluation to the provider and the feds. If the cloud computing provider isn't approved, it will be given 30 days to correct any high-risk vulnerabilities, or 90 days to fix moderate-risk vulnerabilities. Providers must also conduct at least quarterly vulnerability scans of operating systems, Web applications and databases, according to McClure.

Because it will generate income for approved third-party assessors, FedRAMP has sparked much interest from the private sector. "Some of these assessment providers already exist, and some are hoping to be selected and approved," said McClure. "But we'll require both old and new to go through a rigorous certification and review. If they pass, there could potentially be a lot of work available to them."

On Dec. 16, 2011, GSA hosted an Industry Day for vendors wanting to provide cloud services and assess other vendors under the FedRAMP program. The goal of the session was to educate industry representatives on FedRAMP and the third-party assessment application process. More than 200 people attended. During the session, Kathy Conrad, principal deputy association administrator for the GSA Office of Citizen Services and Innovative Technologies, stressed that vendors will be watched closely so as not to violate federal conflict-of-interest rules.

"The success of FedRAMP depends on the integrity and rigor of these third-party assessments. If there is any question that they are not done fairly and consistently and with real independence, that would undermine the whole concept of FedRAMP," she said.

FedRAMP will move into full operations mode in fiscal 2013, scaling intake to accommodate larger demand, according to McClure. By fiscal 2014, it will be in a "sustaining operations" mode, with a mostly automated process in place and JAB will continue to define and update the security authorization requirements. Once launched, FedRAMP will be mandatory for all federal agencies.

"FedRAMP will help us become much more comfortable that the cloud companies will provide the security we need," said Spires. "Even better, it's a leveraged model. Before, there was no way to leverage what one company had done. With FedRAMP, we'll be able to provide that authorization and ultimately should be able to leverage 80 to 90 percent of the work that's already gone on."

McClure said they're also working on securing permanent funding for fiscal 2013 and fiscal 2014, which was originally funded under the e-government initiative. "We are moving to make sure that in FY13 and FY14, we have a sustained budget for FedRAMP parked at GSA," he said.

A Taste of What's Ahead

Why is cloud computing so important to the federal government? VanRoekel's Dec. 8 presentation attempted to address that question. To illustrate his point, VanRoekel included examples of federal agencies that have already used cloud computing to stretch resources. For instance, he pointed out that moving the Environmental Protection Agency's Internet security services to the cloud improved identification of and response to cyberthreats and attacks; tripled bandwidth for Internet connections to support mission requirements; and reduced the cost-per-MB from $179 to $83. Similarly, moving Air Force customer relationship management services to the cloud improved response time (from two to four minutes to two to four seconds); reduced call center volume by 23 percent through better service response; tripled system capacity for queries; and resulted in $12 million in savings.

"I'm excited about saving resources," said Spires. "And FedRAMP should also make it much easier for agencies to launch these services faster. Overall, it will foster a more secure environment for us as we leverage cloud to a greater extent in the future."

It's possible that FedRAMP also may have implications for state and local government. McClure said he thinks that states are paying attention to how FedRAMP unfolds. "If a state or local agency is buying something off the GSA schedule and it's been granted a GSA acceptance, that could mean savings for them if they chose to accept the FedRAMP authorization process," he said. "A lot of them look to the federal process and pattern some of their security processes after ours. It's possible they may duplicate some of our approaches so we end up having the same approach at all levels of government. That would be great, but I don't expect FedRAMP will totally replace what's being done at the state and local levels."

As for the possibility of further delay or even cancelation of FedRAMP, most agree the chances look slim, even with the presidential election on the horizon. "I think we are rolling; at this time, I don't expect any more delays," said TechAmerica's Kerber. "The key thing is to wait and see how the process works and if we can fine-tune it so it's good for both industry and government."

"VanRoekel has been a real champion of FedRAMP," McClure said. " Overall, I think this is a program that will transcend administrations. This program is about good government, and about getting efficient about how we do security reviews. I think we are moving in the right direction, we just have to run it efficiently and do a good job."

http://www.govtech.com/policy-management/Consistent-Federal-IT-Rules-May-Ease-State-and-Local-Cloud-Adoption.html