

FEDERAL NEWS RADIO

Army begins shopping for cloud vendors to host its enterprise apps

By Jared Serbu <<http://federalnewsradio.com/author/jared-serbu/>> January 6, 2016 5:51 am

The Army has started polling prospective cloud computing vendors on their capabilities, laying the groundwork for a new contract vehicle that's likely to handle the lion's share of the service's cloud purchases over the next three years.

A request for information, issued last week, asks companies to describe their approaches to dozens of support services the Army believes it will need as it transitions legacy applications from government data centers to commercially-operated ones between now and the end of 2018, including authentication, network monitoring and the ability to have secondary facilities take over in case of a system failure.

<https://www.fbo.gov/index?s=opportunity&mode=form&id=5bd51582b2244477c7bd0c5ffbd7527f&tab=core&_cview=0>

The overall project, dubbed Army Cloud Computing Enterprise Transformation (ACCENT) still is in the planning stages, but a draft request for proposals released in November envisions a two-step acquisition process in which cloud vendors would first qualify for spots on ACCENT via "basic ordering agreements" but with no guarantee of future work. They would then compete for individual projects at the task order level.

<https://www.fbo.gov/index?s=opportunity&mode=form&id=daff37dab0aff7d1de46e28ac6fc994&tab=core&_cview=0>

Functionally, the BOAs would operate much like the blanket purchase agreements government agencies routinely use to buy a variety of goods and services, said Doug Haskin, the project director for enterprise services within the Army's program executive office for enterprise information systems.

"But we think the BOA is better for the high-dollar contract actions that are associated with hosting services," he said in an interview with Federal News Radio. "It also gives us more flexibility to adapt to uncertain requirements when you don't know all the requirements up front, which is the position we're in now. Keeping that flexibility is important for us because we know that the guidance and policies for commercial cloud in DoD have been changing and will continue to change. I think it's also going to benefit industry, because if they're going to commit the resources to get onto this agreement they need to know it's going to be viable and not obsolete in a year or two."

<<http://federalnewsradio.com/defense/2014/09/dod-upends-its-strategy-for-buying-commercial-cloud-services/>>

The Army envisions using the contract to buy infrastructure-as-a-service, platform-as-a-service and software-as-a-service cloud offerings. Vendors would need to meet the government wide FedRAMP standards for cloud security and have DoD-specific provisional authorizations to sell their wares to the government, but the additional DoD security controls they would need to comply with would be set out task order-by task order.

<<http://federalnewsradio.com/disa/2015/09/dod-reaches-36-provisional-authorizations-commercial-cloud-services/>>

Additionally, companies would need to support DoD's public key infrastructure to authenticate users via their common access cards, make sure all the government data they're hosting is physically stored in the U.S. and be willing to open their facilities to DoD security teams at any time in case of a cybersecurity incident or criminal investigation. And under task orders issued for DoD's highest unclassified cloud security designation – Level 5 – all government data would have to be kept physically separate from that of the hosting companies' commercial clients.

The Army plans to use the ACCENT contract to follow through on guidance the service's chief information officer issued last July, telling all Army components that they had until 2018 to migrate as many of their enterprise-level applications as possible to commercial environments.
<<http://ciog6.army.mil/Portals/1/CloudStrategy07312015.pdf>>

In turn, the commercial cloud migration strategy is only one element of the Army's broader data center consolidation initiative, which it's been working on in fits and starts since 2011. The service intends to use the Defense Information Systems Agency's MilCloud service for applications that are deemed too sensitive for commercial hosting. And at Redstone Arsenal, Ala., officials are piloting the idea of secure, commercially-operated data centers on military bases.
<<http://federalnewsradio.com/army/2015/09/army-test-commercially-run-cloud-services-military-bases/>>

Still other applications will escape Army mandates to migrate to enterprise data centers, as long as they only serve users on one base. They will be maintained in local "installation processing nodes."

"We're going to have both on-premise and off-premise components," Haskin said. "It's a multifaceted approach, not a one-size-fits-all. We've taken that direction in the past and we've found over the years that it's best to take a more balanced approach and not put all of your eggs in one basket."

For now, the Army is focused on moving as much of its unclassified data as possible into "true" commercial off-premise data centers, Haskin said, while preserving the option to use some type of vendor-provided services for sensitive or perhaps classified data in the future.

"The intent is to run the pilot at Redstone and use that to get some of those sensitive systems in there and test it, because we wouldn't want them going into an off-premise commercial cloud right now," he said. "We'll learn the lessons from that and use those in the future when we roll this concept out Armywide."