(http://federalnewsradio.com)

In Pentagon's belated march to the cloud, DoD CIO looks to spark 'national dialogue' on cloud security

By Jared Serbu (http://federalnewsradio.com/author/jared-serbu/) | @jserbuWFED (https://twitter.com/jserbuWFED)
January 30, 2015 12:17 pm

The Pentagon's top technology official told vendors Thursday that DoD wants a much closer partnership with commercial cloud providers, and that the department is destined to put much more of its data into privately-hosted computing environments.

The cybersecurity worries that have made the military a reluctant adopter of cloud computing are far from resolved, so far. But Terry Halvorsen, DoD's acting chief information officer, said his department is determined to overcome them. For starters, the department's public-facing websites should be turned over to cloud providers post-haste, he said, and the military's email services ought to be managed by IT firms who do that sort of thing for a living.

Terry Halvorsen, acting chief information officer, DoD

In the first of what he vowed would be many more industry engagements surrounding DoD's use of commercial IT services, Halvorsen outlined the broad strokes of an agenda that would attempt not only to bring the department up to speed with cloud computing, but also seek to influence the way all cloud services — both public and private — are secured in the future.

As its own new starting point, DoD released a new security requirements guide two weeks ago which more clearly delineates its security demands from cloud service providers, and recognizes that not all data is created equal.

"What's really the right level of security for things like financial data or personnel data? If we get those answers right, that's way beyond just what we can use in DoD," Halvorsen said. "All of you want your data to be secure too, and you in industry ought to be asking where your data is, because a lot if it is not very secure. If we can raise that national bar together, we can do it much more effectively and much more efficiently."

DoD formally revised (http://www.federalnewsradio.com/405/3780452/DoD-rewrites-cloud-security-rules-in-move-toward-risk-acceptance) its approach to cloud security in a newly-published security requirements guide earlier this month, simplifying some of the demands the department imposes on cloud providers, streamlining some of its processes and aligning its procedures more closely with existing standards for cloud security. Cloud providers who have already met the governmentwide FedRAMP standards (http://www.federalnewsradio.com/473/3752146/FedRAMP-developing-a-FISMA-high-baseline-in-2015) are eligible to handle DoD's less sensitive "level 2″ data without any additional security requirements.

For now, the department is requiring a DoD-only “FedRAMP Plus” certification process that adds more checks when vendors are dealing with more sensitive data. But Halvorsen said there’s no good reason it has to be that way forever.

“If we get FedRAMP Plus right, that ought to become no longer just our own ‘plus’ requirement, we could have a national standard that is not just for the government, but that applies to everybody,” he said. “It would say, ‘Okay, if you’ve got this type of medical data, this is the level of protection it needs.’ Commercial, government, academic, anyplace, we ought to have that that level of protection so that it’s not overprotected and it’s not overpriced. I think we can get a national dialogue started, and I think this group of people here can actually do that.”

The Defense Department has only a handful of companies in its catalog of approved cloud computing service providers so far. While it hopes the revised procedures will expand the crop, Halvorsen is also thinking a few steps ahead.

DoD’s path forward will require a shift in risk acceptance. In certain cases — like military installations’ mess hall menus and budget data from 1942 — the department is probably applying more security protections than the cost justifies, Halvorsen said. On the other hand, some providers will be taking care of genuinely relevant national security information, and that might require some innovative partnerships. Like letting companies build their data centers on military bases.

“I have still not taken off the table that at one point we might have a data distribution center that is mostly contracted, but inside a government installation where we provide the physical security,” he said. “We have some advantages there: most physical security people can’t roll tanks up to your building to help out. We can do that. Government does some things really well. How do we do that partnership? It takes some different thinking, it takes some different acquisition approaches.”

Speaking to reporters on the sidelines of the industry day, Halvorsen said that the private-data-center-on-government-facility approach is still just a notion. But he also sees it as one way to lower the overall cost of cloud computing while also increasing security.

“We’ve actually done some of that already, but not to the level I want,” he said. “In the department of the Navy, Hewlett Packard operates some of their own data centers inside federal space. The arrangement is good, but I’d like to push it bigger. For example, HP doesn’t store anybody’s data in there except ours. My model would say, ‘Why couldn’t HP do that, but make money by storing other companies’ data?’ If you’re a defense contractor,

you really have to play by my rule sets. Maybe one of those contractors would like to put their data into one of those facilities that's already in a very secure place. The other group I see that would want to do that is financial institutions.

We are not there yet, but that's what we're looking to push the model forward on."

Before pulling off anything that bold, DoD needs to start with the basics, like putting policies in place that let it migrate meaningful quantities of data and processing capacity into commercial cloud environments. The security guide it published this month eased that process for data that's already publicly releasable, and Halvorsen says that's where DoD components need to start.

"This ought to be a no-brainer," he said. "For all of us in the government, if we have data that we want to get to the public — our marketing and information exchange with the public — why wouldn't we put that in a public cloud? The public might actually be able to see it then. One of our problems sometimes is we have public-facing data sitting in our own networks, but, small problem, the public can't get to it. If you put that in a public cloud, not only do you get a cost advantage, you get some mission effectiveness right away."

More mission effectiveness, officials say, because DoD's owned-and-operated systems would be relieved from having to host and handle data that doesn't need to be protected to the military's high security standards.

"Pushing anything that's public facing out to commercial industry really helps me out," said Maj. Gen. Alan Lynn, the vice director of the Defense Information Systems Agency. "Because I really want to have a highly-secure platform for DoD, and the more I'm touching the outer surface of the Web with my networks, the more risk I take. So anything we can push out to the commercial space is a boon for our business."

Beyond public websites, Halvorsen said DoD plans to start pushing a host of other less-sensitive computing responsibilities into commercial computing environments, including all of the department's unclassified email.

DoD started consolidating (http://www.federalnewsradio.com/405/3741453/Armys-move-to-enterprise-email-kicked-culture-transformation-into-gear) many of its unclassified email systems into a single "enterprise email" system several years ago, but for now, it's hosted and operated by DISA. Halvorsen has told the agency that the next version — Defense Enterprise Email 2.0 — needs to be an entirely commercial endeavor.

“I think that the commercial industry has certainly shown that they could do an unclassified email system at a lower price, and that shouldn’t surprise anybody,” he said. “Email is commoditized. So any time you can share in a commoditized environment, you’re going to drive down the price, and I think they’re at the point where they’ll be able to meet our security requirements. Again, I see the national cyber bar coming up, and I think that we’re such a big market that they’ll willing to adapt their security to meet our needs. I’m hoping this comes out to be 25 to 30 percent more efficient when we’re done.”

But Defense IT officials say they’re not standing still when it comes to incorporating cloud into hosting and processing needs for sensitive data. Under what the new security guide categorizes as levels 4, 5 and 6 information, cloud providers will have to interact with DoD-operated “cloud access points” that apply Pentagon security protections to data that moves back and forth between the cloud. Those access points don’t exist yet, aside from two pilot programs being run by DISA and the Navy. But Halvorsen says they’re coming soon.

“When I get that right, I actually further reduce my security problem,” he said. “Some of it is just about physical footprint. If I have fewer points where I connect to the broad commercial network, it’s easier to secure. DISA is moving very quickly — this is actually one place where I’m happy with the movement. We can’t tell industry the exact solution yet, we really have to make sure we’ve done the right threat analysis. But I suspect that within the next 90 days we’ll be able to start standing up the cloud access points.”

RELATED STORIES:

DoD rewrites cloud security rules in move toward risk acceptance (http://www.federalnewsradio.com/405/3780452/DoD-rewrites-cloud-security- rules-in-move-toward-risk-acceptance)

FedRAMP developing a FISMA high baseline in 2015 (http://www.federalnewsradio.com/473/3752146/FedRAMP-developing-a-FISMA- high-baseline-in-2015)

Army’s move to enterprise email kicked culture transformation into gear (http://www.federalnewsradio.com/405/3741453/Armys-move-to-enterprise- email-kicked-culture-transformation-into-gear)

INSIDE DEFENSE

DefenseAlert

Army Taps IBM Cloud Computing To Help Manage Its Logistics Enterprise

The Army has connected IBM cloud computing services to its own systems powering the Logistics Support Activity to better manage the vast amount of transactions processed every day, the company announced.

The "hybrid" cloud system, a reference to a computing environment that retains Army-specific elements, would enable the use of improved analytics, better performance and greater security, according to an April 8 IBM statement. The service stands to save 50 percent in costs, the company contends without providing details.

"The Army not only recognized a trend in IT that could transform how they deliver services to their logistics personnel around the world, they also implemented a cloud environment quickly and are already experiencing significant benefits," Anne Altman, general manager for U.S. Federal at IBM, was quoted as saying in the statement. "They're taking advantage of the inherent benefits of hybrid cloud: security and the ability to connect it with an existing IT system. It also gives the Army the flexibility to incorporate new analytics services and mobile capabilities."

According to IBM, the Army's Logistics Support Activity processes 40 million unique data transactions every day, which is more than the number generated daily by the New York Stock Exchange.

Service officials last month defined their way ahead in cloud computing in the first version of a strategy document devoted to the technology. The strategy promulgates that much of the Army's IT portfolio is now tied to cloud computing.

"The Army is changing its approach to modernizing information technology infrastructure by moving to a cloud-based approach," the document reads. "This approach emphasizes reducing IT hardware procurements and sustainment in favor of procuring these capabilities as services from cloud providers."

At the same time, service Chief Information Officer Lt. Gen. Robert Ferrell acknowledged the potential pitfalls of the technology in a foreword to the strategy.

"The potential vulnerabilities of, and impacts to, expeditionary operations in highly contested and inevitably degraded communication environments must be carefully and continuously assessed and weighed against the advantages of adopting cloud technologies," Ferrell wrote.

The "dramatic, yet very necessary" move toward cloud computing environments would require "support of every corner of our Army," the document states. -- Sebastian Sprenger