Washington Technology

SPONSORED BY Microsoft

DOD Enlists the Cloud

Cloud computing fits well with the department's focus on business outcomes.

Moving operations to the cloud dovetails well with the Defense Department's ongoing strategy. The goals are to make its business functions more efficient and free up money for higher priority programs. However, it will require some major changes within the department, including rethinking its policy, contracting, and business processes.

The DoD wants to reduce duplication, save money and improve its overall mission outcomes. This means taking a fresh look at areas where cross-enterprise consolidation makes sense, such as human resources, financial management, acquisition, and IT management.

"We want more bang for the buck," says John Bergin, Business Technology Officer, DoD CIO, DoD, speaking at a May 12th event. This includes embracing cloud computing and shared services—technologies that have matured over the past few years. "Seven years ago, I would have been up here convincing you that logical separation in a hypervisor could be secure. I don't have to do that any more."

The DoD wants to work with industry to help it come up with solutions, including building a business case and addressing total cost of ownership issues. Where industry has solved a problem for a large bank or large pharmaceutical company, the DoD wants them to, "come back and help us solve that problem too."

There are areas where DoD wants to establish partnerships, but it also plans to leverage its size to negotiate better prices for technologies such as mobile devices. The goal is to "find a happy middle ground."

CULTURE CHANGE

It's no longer business as usual within the DoD and cloud is a reflection of that, says Victor Gavin, Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers, Intelligence, Information Operations and Space, US Navy. "I believe our move to the cloud is the most fundamental change that we have had in DoD since our migration to COTS technology," he says, speaking at the event.

It's time for the department to focus more on outcomes and less on products. "We have to get away from buying the product to buying the service," he says, "and allow those changes to take place within that contract structure." DOD struggles with how to best handle this change, particularly as it relates to acquisition and security, but it must embrace it and evolve. "We can't stay in the past."

Success will rest in part on changing the culture of the department, says Gavin, because "culture eats strategy for lunch." He hopes industry can help the department not only understand the technology and business case for cloud, but also the proper role for the department in the relationship.

Vendors appear ready to help agencies move to the cloud, according to industry speakers at the event: Defense Contracting: Delivering on the Demands of Secure Cloud for DOD. "Our job is to improve the user experience for core mission to allow them to stop thinking about IT and to do their mission," says Larry Prior, President and Chief Executive Officer, CSRA. This will require change management from within the department, but because of the scalability, flexibility and potential cost savings cloud offers, the effort will be worthwhile.

> **"IT has to match the pace of the mission as opposed to the pace of policy."**
>
> **—Larry Prior,** President and CEO, CSRA

Industry can help agencies manage the complex cloud pricing model and make a strong business case for cloud, says Prior, but departments will have rethink policy and strategy. "IT has to match the pace of the mission as opposed to the pace of policy," he says. CSRA is in every FedRAMP high cloud and has selected Microsoft Azure Impact Level 4 for many of its workloads in anticipation of where the DoD is headed with secure cloud. The company is also DFARS compliant.

Microsoft spends more than $1 billion per month globally on its cloud infrastructure. It was the first cloud provider announcing support for DFARS controls, says Tom Keane, General Manager, Microsoft Azure. With Azure, Microsoft is providing agencies with mission capability. "I'm not just providing ... very secure technology, or (an) elastic infrastructure," says Keane. "I need to be helping you solve an end-to-end mission."

The cloud is increasingly taking off in sectors such as defense, government, and intelligence, says Keane. Microsoft is committed to the cloud not just from an investment perspective, but also from a security and compliance perspective as well. For example, Azure covers 58 compliance offerings, such as DoD SRG Level 5 compliance.

The cloud helps Microsoft provide innovative products as well, such as the company's Azure N- Series virtual machines that can process imagery in real-time. The product can pull data from multiple sources, such as facial images, voice recognition samples, metadata information and biographical data, to help identify a person or image.

"We're sourcing all this information together to give a single, unified view of these individuals," says Steve Michelotti, Chief Evangelist, Microsoft Azure Government. The system can also analyze video from a security camera, index video to look for key words and faces, and produce a live transcript. "We can bring these cognitive services together to build really compelling applications."

> **"You will need to look at the big picture and look at security quite differently than we do today."**
>
> **—Susie Adams,** Chief Technology Officer, Microsoft Federal

SECURITY IN A VIRTUAL WORLD

The industry is on the cusp of a fourth industrial revolution and cloud and mobile technology are driving it, says Susie Adams, Chief Technology Officer, Microsoft Federal. The challenges agencies face with cloud and mobile will "go well beyond the constructs of FedRAMP compliance in the cloud," she says. "You will need to look at the big picture and look at security quite differently than we do today."

Organizations will have to learn to protect a perimeter-less virtual environment and their data wherever it is located. "Identity becomes the new firewall and you need to protect data regardless of where it lives, and that includes the cloud," says Adams.

Cloud gives agencies the ability to look at big data to not only better serve its citizens, but also better protect its systems. Cloud supports auto data classification and provides visibility into where data located and who has legitimate access.

Compliance is important, but it is not the same as security, says Adams. What outcome are agencies trying to achieve? They should apply rigid compliance on top of how to implement a control, she says. Agencies have to evaluate security, compliance, trust, and cloud capabilities, and determine how to bridge the gap between data that must reside on-premises and data that can be in the cloud. Azure makes this easier for agencies to achieve.

Some cloud vendors offer a complete cloud package and some just provide components. Agencies will need to fill in those gaps to ensure security is sufficient, says John Connor, IT Security Specialist, Office of Information Systems Management, NIST. "When you're looking at cloud vendors, make sure you understand the scope of where your data is and who has access to the data," says Connor.

FedRAMP is a great resource, but the onus is still on agencies to review the package and make sure it encompasses the scope and capabilities agencies require. For example, agencies should understand protections around data stored at back-up sites because they can be a weak link.

Industry plays a role in helping the DoD determine the appropriate level of data protection and whether additional assessments are necessary, says Kevin Dulany, Chief, Risk Management Framework Division, and Deputy CIO for Cybersecurity (DCIO-CS), DoD. The DoD must also forge a relationship with other data owners to "bring the feeder pieces in."

Cyber security is now an "enabler to mission accomplishment," which is a shift from how it's been viewed in the past, says Dulany. With the focus on outcomes, the DoD must determine how to apply the "appropriate IT or technologies needed to support the business process."

It is also a challenge to deliver cloud technologies to DoD tactical users who don't have broadband or access to the data center, says Thomas Sasala, Director, Army Architecture Integration Center, Office of the Chief Information Officer/G6, Army. "How do you do the same thing, at the same time, at the same speed, when you don't have a network and you have a satellite communication that is contested?" he says. This is a problem the DoD hopes industry will help it solve, which will depend on developing a strong relationship built on trust.

Vendors should work together as well by combining their areas of expertise, such as developing a special forces application, with another vendor's cloud infrastructure, instead of starting from scratch, says Sasala.

Industry can help the Army move away from Army-only environments, centralize its data centers and focus on defense-in-depth. Ultimately, the service wants to establish an environment to understand the data itself and become "data aware." Cloud gives it the compute capacity and agility to do this.