Event Summary: Merit-Based and Competitive Awarding of Federal IT Services: Public Policy and Department of Defense Cloud Computing

Participants:
- William Schneider, moderator, Senior Fellow, Hudson Institute
- John Stenbit, Former Assistant Secretary of Defense for Command, Control, Communications and Intelligence, U.S. Department of Defense
- Stephen Bryen, Former Director, Defense Technology Security Administration

On April 12, 2018, Hudson Institute convened a panel discussion on "Merit-Based and Competitive Awarding of Federal IT Services: Public Policy and Department of Defense Cloud Computing."

This event summary addresses the major issues discussed by participants during the conference and draws on the full transcript of the event, available here: https://www.hudson.org/research/14276-transcript-merit-based-and-competitive-awarding-of-federal-it-services-public-policy-and-department-of-defense-cloud-computing

Hudson Institute is grateful for the support of Oracle Corporation in sponsoring the event and associated publications.

Hudson Institute
1201 Pennsylvania Ave, N.W., Suite 400
Washington, DC 20004
April 12th, 2018
Background to the Joint Enterprise Defense Infrastructure (JEDI) Procurement

The current effort of the U.S. Department of Defense (DoD) to "move to the cloud" is the latest manifestation of the exponentially growing role of data in military affairs. Between the Gulf Wars, bandwidth was beginning to substitute for force structure in the allocation of force against targets. We're now at the front end of the evolution of the way in which DoD conducts military operations to be increasingly dependent on data. The poster child for that, of course, is the F-35, whose operation depends fundamentally on access to data that is not housed on the plane itself.

In the private sector, companies that use cloud-based services typically have eight or so different providers because of the nature of the competitive landscape and the fact that there are many different forms in which cloud computing takes place. The underlying technologies creating the cloud services are evolving at differing rates and have different applications depending on the needs of the user. So it's a very vibrant market. And the question is, how can DoD take advantage of this?

This is very consistent with the dilemma that DoD is facing every day. To an increasing degree, military performance depends on technologies that are not produced in the defense sector. They are largely of commercial origin and adapted to defense applications. And certainly, cloud-based services are an illustration of that trend.

There are a lot of industry lessons learned that DoD can exploit. In commercial practice, you can have the convenience of a single provider or the complexity of managing multiple providers. If you select the latter, presumably it's because the industry is quite vibrant and has produced many alternative ways of delivering services based on the needs of the user. It's quite common for industry to have multiple providers that offer different types of services and are able to reflect a process of more continuous innovation. In the case of cloud-based architecture, new providers may have different ideas about security or process efficiency. There is room for some experimentation here. And DoD may not be availing itself of the opportunity that it has by failing to look at alternative ways of procuring cloud services.

Private Sector vs. DoD

Private sector use of cloud is usually in multiple providers. And why is that? Is it for budget reasons, or is it because of better capacity in reliability, availability, stability and dealing with problems? If the general trend is to have multiple providers, then one has to think it's not just for money, but because it's the pragmatic and operational decision that makes the most sense.

DoD has created an ad hoc mechanism to facilitate the rapid procurement of cloud services. That has a lot of positive features, in that it focuses leadership attention on a problem and makes it more likely that the operation will get the resources it needs. But it also has the property that it narrows the aperture of sensitivity to the kind of concerns raised here and hence contributes to the risks that you won't have the outcome that DoD both needs and seeks.
What Is "the Cloud"?

"Cloud" is not a noun. Cloud computing is different from cloud storage, which is different from cloud operation. The "cloud" is not a piece of hardware in the sky. It's a series of systems that provide three basic types of services, all different. And they need to be applied to different problems. We tend to think about crypto and cyber and a whole bunch of other issues, but it's really information operations. Information operations have to do with denying the other person the ability to work. In electronic warfare, that's called jamming. In cyber, it's called a denial of service (DoS) attack. They're the same thing, but the people who do it don't think the same way. And they should because there's a lot to learn from both sides.

Cloud services need to be considered as part of the system they support. Cloud services need to be "system engineered" so that their data storage, processing, and operations applications are optimized for the system they will support. Procuring cloud services independently—outside the system in which cloud-based applications will be performed—would ensure that cloud services themselves are integrated (because one contractor provides the hardware), but will not produce an optimal outcome for the function performed by the entire system, of which cloud-based services are only a part.

To facilitate management and financial oversight, the process of authorization and appropriation of federal funds for national defense is divided among thousands of "program elements." This approach reflects the organization of DoD in the industrial age, but it is not effective for the information age. Information needs to be integrated to provide insight and value to DoD's military and civilian leadership. Parallel "stovepipes" of information developed by elements of DoD’s activities need to be integrated to allow DoD leadership to extract value. To provide the insight DoD leadership needs, information needs to be integrated, not split.

The information-splitting problem again suggests an alternative acquisition model in which these issues can be identified and worked out before the new cloud services are widely propagated. Once again, DoD has the opportunity to take advantage of the vibrancy of the industry and the rapid technological change that's taking place with the enabling technologies supporting cloud-based IT. Doing so would seem to be a way of reducing the systems-engineering risks that DoD would take with a highly centralized platform for its data storage, processing, and operations.

Security Issues

As the Internet was propagated through DoD, the decentralized model of computing turned out to pose a grave risk of loss of data. And, in fact, discussions have been had at DoD about whether it's possible to conduct a war properly without any security. Because when you have a situation where terabytes of data have been taken from highly classified storage, it does suggest that the imperative of security has to be at the forefront of moving to a cloud-based architecture.

The greatest example of failed IT security is the compromise of the data for the F-35 program, where some 50 gigabytes of information disappeared, probably to China. Security is definitely an issue, and so is cloud security. It's not true that the cloud is secure. There are many cloud providers, and some of them...
have had incidents already, serious incidents. You can ask Tesla about that—their system was actually deployed on the Amazon cloud, and it was hacked.

The cloud industry is a growing industry. This year it will be about $160 billion in this country. A lot of money is going into it because it offers efficiencies, especially for businesses—although most businesses have chosen to have multiple cloud providers as a way of providing some backup to risks that are inherent in depending on one provider.

The DoD procurement is proposed as a multi-billion-dollar procurement for 10 years, but only to one provider. It leaves open the question, what's the backup? And that is not clear. If you could do a denial of service attack on a cloud, which is one risk, and shut it down, you could shut down DoD. So the backup is likely the existing system, and we know that it's not adequately secure.

Where is the risk assessment? This whole "move to the cloud" looks like standard procurement—with all these unsettled issues swarming underneath. No one's paying attention, and that's scary.

Now, for the procurement that we're discussing, DoD has laid down its own standards or guidelines on what it expects the security of a system that it's going to procure should look like. And what they've done, for the most part, is two things. One, of course, is to make sure the employees who are working in the proposed cloud environment are cleared Americans. That creates a significant problem. Enough cleared American employees may not be readily available.

The second thing they've done is to take the procedures that are used to secure DoD's existing computers, servers and equipment—the Security Technical Implementation Guidelines (STIG)—and apply those standards to the cloud. So it's a question whether DoD has confidence in these standards. Basically there are about 400 STIG guidelines—a massive checklist that you go through to make sure you're in compliance. So if there's a known vulnerability, you're supposed to check that off and make sure it has been addressed, and basically to do this once a year for every computer. The problem is not everybody does it once a year for every computer. About 25 percent of them do it, and the rest of them don't. They apply for exceptions because a lot of the STIGs require taking down the system to check it, and if you take down the system, you don't have it operational. So how you would follow these procedures in a single-cloud context is unknown. That's a serious, serious problem because they're not going to be able to take down the cloud to fix a vulnerability.

You can see they just imported the procedures they already have—nothing new, just the system in place—to the cloud. They don't have a STIG that really is addressing cloud issues, which have a lot of management systems that don't exist in DoD systems. So it's very clear what the situation is, and it's troublesome.

Another area of concern is that the architecture of these systems is not confined to our borders. The supply chain that supports it is all over the place, mostly in Asia. And our friends in China have supercomputers now that are even outperforming the supercomputers we have. We're setting ourselves up for a lot of trouble by migrating to a kind of generic system without studying it fully. It's not that we shouldn't use cloud technology, but we should carefully study the implications, because we know very well the Chinese are not only extraordinarily active in this field, they're also good at it. But to operate
with Chinese entities and Chinese companies, China requires cloud providers to hand over not only all the information about their systems, but also the encryption keys. So there's a lot of risk here that doesn't seem to have been fully assessed.

**Mission Issues, Including Experience with IC ITE (Intelligence Community Information Technology Enterprise) and Allies**

The Intelligence Community (IC) went wholeheartedly into a cloud monoculture, and DoD seems interested in trying to replicate the Intelligence Community experience. There are a lot of reasons, however, why that may not be an appropriate model for DoD—because of the different missions that they have.

It's very important to worry about how cloud processing, cloud storage and cloud operation interface with each other and then with users. Because every one of those interfaces is going to be different. Unfortunately, the government is not very good at system engineering, which is a process of taking various problems and solutions and putting them together.

And the engagement appears to be binary—the DoD seem to have gone extremely rapidly from monitoring the IC's progress with cloud services and thinking about it to a decision about DoD's own procurement.

This is an area that's been moving along for several years without DoD really engaging. DoD has elected to move very quickly, but DoD is not well organized to move quickly on things. So sometimes you produce the "want-it-bad, get-it-bad" kind of outcome. And that raises the additional risk of how to recover from a bad outcome. What are alternative acquisition models that might be undertaken to facilitate a recovery?

The problem with the IC cloud (Commercial Cloud Services, or C2S) was that the people who did the joint desktop environment (Common Desktop Environment, or DTE), at the National Geospatial-Intelligence Agency (NGA), didn't pay adequate attention to either National Security Agency (NSA), Central Intelligence Agency (CIA) or DoD requirements. The cloud operation didn't work because it was not interoperable. It's a classic problem: you need alternate sources. You need to protect yourself by not standing still, and hiding yourself. You have to do all kinds of things to protect yourself in this world. You can run a pretty good enclave of pretty secret people. Both DoD and the Intelligence Community know how to do that when they have sufficient freedom with regard to the processes they employ. If they get forced into a generic cloud, they'll have a much harder problem to solve.

If we're going to inter-operate, whether with tactical aircraft or the more recent decisions on U.S., Japanese and South Korean missile defense collaboration, we will need to have the appropriate data integrated and operated in near real time. That's the nature of the problem. We need to be thinking about how to manage this data in ways that contribute to the security of our allied partners as well. Look at the discouraging example of the Libya campaign, where the U.S. made a decision not to lead. That produced a lot of unhelpful outcomes because of the inability of the allies to share data and to use it in constructive ways. When we're considering how we're going to manage the movement of DoD data to the cloud, we
need to be thinking about how we will engage our allies and how we will manage that interface so that we, as an alliance, can have high confidence that we'll be able to achieve our military aims as efficiently as possible.

**Competition Policy Issues**

The cloud, whether it's processing, operations or storage, is the sharing of resources such that you're not overloaded or under-loaded. In other words, if you don't have a constant information load, you can save money by sharing. Let's say you're doing a biochemical modeling of DNA. It takes an enormous amount of computing power for a very short period of time. The cloud allows you to sign up for that enormous amount of computing power. And then five seconds after you're finished, you turn it off and don't pay any more. Money always matters. But you've also got to worry about what your system does.

When General Clapper was Director of National Intelligence (DNI), he specifically expressed the view that the Intelligence Community could save about 50 percent of its IT budget by going to the cloud. They were looking at a very steep ramp for costs if they didn't do something like that. Driven by budget circumstances, you want to believe. The intelligence cloud was clearly there because of the squeeze in money. The claim was that the intelligence cloud would save $108.72 million per year. And the money was spent—up front—and the savings didn't come.

Congress has been the big driver in promoting competition in federal contracting, and there is a presumption that DoD procurements will be competitive. Both DoD and the industries providing services to DoD have generally been well served by competitive procurement, because (unlike for military hardware) the industry has tended to be quite vibrant, with large numbers of participants in the market.

The DoD procurement process needs to take advantage of the dynamism of the industry, which is technology-driven. There are many dimensions being altered, enabled, etc. Different cloud service providers will offer different services. DoD, in an effort to maintain a posture of continuous innovation, needs to find a way to manage that. A single service provider may not be the way.