Hudson Institute

Event Transcript:
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*

The event was held on April 12, 2018, at Hudson Institute's Walter and Betsy Stern Conference Center in Washington, D.C. Additional details and a video recording of the event can be accessed here: https://www.hudson.org/events/1542-merit-based-and-competitive-awarding-of-federal-it-services-public-policy-and-department-of-defense-cloud-computing42018

Please note: This transcript is based from a recording and mistranslations may appear in text. The names of participants in the Audience Q&A have been removed.

Hudson Institute
1201 Pennsylvania Ave, N.W., Suite 400
Washington, DC 20004
April 12th, 2018

WILLIAM SCHNEIDER: I think we'll begin. And I'd like to welcome all of you to this meeting and discussion. And we are going to emphasize the discussion. This is a - the subject we're discussing concerning the merit-based acquisition of cloud computing services is a current issue. It's likely to be an enduring one because of the fact that the Department of Defense is moving decisively into the domain where data is a dominant enabler of military performance. You think back almost three decades, in Operation Desert Storm - first major military campaign after the end of the Cold War. We went in with over 300,000 troops and 360,000 MILVANs full of equipment. A dozen years later, in the same theater, we had about half as many troops and half the logistics burden but engaged in a much wider area. What you saw over that intervening period were the military applications of information technologies. Loosely speaking, bandwidth was beginning to substitute for force structure in the sense that the bandwidth gave you the opportunity to have much more efficient allocation of forces against targets, and that contributed to reducing the burden. What we're now at the front end of is the evolution of the way in which the Department of Defense conducts military operations to be increasingly dependent on data for being able to do so. The sort of poster child for that, of course, is the F-35, which is vitally dependent on sources of data that are not in the aircraft, and hence the need to acquire data to be able to successfully conduct military operations with that advanced piece of equipment.

But as those of you who are close to defense R&D will almost certainly be aware of the extraordinary efforts being made to couple access to data to almost every dimension of military operations, from close combat to logistics operations. And we're just - because we're just at the beginning of this, the public policy questions about how the DoD should procure services that will enable it to draw from the pool of data that the military operations are creating and be able to exploit – that is an issue. The underlying technologies for the use of cloud-based services is now a widely established commercial venture. A typical company that uses cloud-based services typically has eight 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. And there - the underlying technologies that are 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 the DoD has faced - is facing every day, where to an increasing degree, military performance depends on technologies. They're 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.

So for our discussion today, we have two people who have been very active in various phases of this revolution in military affairs that has made data a central element of the way in which we create military capabilities and the way we conduct military operations. To my right, your left, is John STENBIT, who many of you know from his service in the Department of Defense, where he was assistant secretary for C3I and is extraordinarily knowledgeable both from the government end but also in the private sector, where he's served in major corporations that have been innovators in these areas as well. And to my left, your right, Steve BRYEN, a colleague of mine from both congressional staff and DoD government service. Steve was formerly the director of the Defense Technology Security Administration - indeed, the first incumbent to that position - and has been also a commentator on advanced defense technology for more years than he would care that I mention. So - good, so the aspiration is to really stimulate a discussion. This is a front-burner public topic. And for many of you who are already industry practitioners or in various ways involved in the sector, we would like to engage because this is a public policy project.

We're trying to understand what is the best way forward. So I'll start with John, and he'll - you know, he'll make a few brief comments, followed by Steve and then I'll open it up for discussion.

JOHN STENBIT: I thought it might be interesting to give you my perspective of the evolution of the information applications in the DoD. I first went in the DoD in the '70s. We'd just had the Pueblo captured in North - by North Korea. And that was a major information failure. And it was based fundamentally on how we did information. If you want to think about it, the thing to think about is a telephone. And if somebody had something to say, they needed to know that it was important. So they had to be smart about that. And they needed to know to whom to send it. And so what happens in that kind of a case is that bandwidth is expensive; processing is expensive. It's all in a controlled sort of environment. So it's synchronous in time, synchronous in space. The DoD didn't have answering machines. So if you called and they didn't answer, that was it. So there were a lot of private lines connecting things back together. But now let's go to Commander Bucher, who's on the Pueblo, and the North Koreans come after him. And he says, oh, my God, this is important. So he's smart. He knows it's important. And what he's got is a list of telephone numbers, all of whom are spooks that work for NSA. Nobody owns a gun or anything else on there. He was dumb about how to get those data out. And the result was it took four days for the Washington bureaucracy to get itself together and talk to each other and figure out it all. And then somebody said, hey, we have F-4s on Okinawa. We could get there and intercept it. Except the North Koreans had it back in port in 30 hours. And he stayed there for a year...

SCHNEIDER: Yes.

STENBIT: ...Or something like that - a miserable failure of the telephone model. And we're coming into the mid-'70s - lots of issues all over the place. That kind of a system wasn't going to work anymore. We had a new - we had a new technology. It was basically called satellites. It was an expensive way - bandwidth was still very expensive, but it covered sort of the whole earth. So it's called directed-broadcast information. So let's just divide the world into people that find targets and people that have guns. In the telephone model, you had to be right next to each other. And you said, I'll take the guy on the right; you take the guy on the left. And there was no way to coordinate amongst organizations without a lot of trouble. The only place that happened was at the Strategic Air Command, where they had a national plan for using nuclear weapons. And if you wanted to change it, it took two years - an enormous amount of processing to get all of that done. So that was not going to be the right thing.

We switched to a system, which is broadcast. Somebody has some data about a target, he sends it to a satellite. Somebody has a gun, he listens to a satellite. So now we have - processing is cheaper because you have to have lots of people listening to satellites, lots of people transmitting to satellites, but bandwidth is still very expensive. But what it does is it allows the person who's got the gun not to have any particular knowledge of the other guy. GPS helps all of this. And it helps - the guy who has the data doesn't have to know anything about who's doing what. So he sends it up. The best example - by the way, that's in the '70s. The intelligence community came onboard in the '80s. And we first used that in Iraq in 1991. But the one I find to be the most interesting because we'd really refined it by - when we went in Afghanistan in 2001. I don't know if you remember the story about the special ops guy on the camel with the Northern Alliance people. And he sees some bad guys over there on this hill. And he says, I need a bomb on that hill. And within a couple of minutes, the hill blows up. He had no idea who was going to

send the bomb. The guy on the - in the airplane didn't have any idea where the thing was coming from. But it was this connect-the-people-that-find-the-data-to-the-people-that-have-the-gun.

When I went in this time, we were very good at this system now, except there's a problem. So now we have the Internet. And we don't have to be smart-push, smart-pull, all the rest of it. We can just have the person who needs the data pull it. So if somebody takes a picture, and NGA processes it and posts it, then it gets sent to various people. But it's on their website, and you can go retrieve it, if you have the proper credentials, by saying what area of the world you want have a picture of. That gets fouled up when we were in Afghanistan and Iraq at the same time, and somebody has come down to the director of NGA one day and said, Iraq has a higher priority than Afghanistan. Now, you'd think actually that you should be able to do the highest priority in Iraq and then the highest from Afghanistan and so forth. And that's not how government bureaucracies work, in case - certainly not I've observed. So the last picture from Iraq gets done before the first one in Afghanistan. That's next day.

If you're the captain in Afghanistan and there's a picture already taken about the other side of the hill but you can't get it because the bureaucracy is not going to process it till tomorrow, you are angry, OK? If it's on the Internet and NGA posts the pictures, from which their analysts grab it to do their stuff, then that guy in Afghanistan can pull the same thing and use Photoshop to look on the other side of the hill. It's a totally different way to think about how it goes. We're not doing a real good job of that these days. There's a lot of moving around. There are a lot of ad hoc ways that are being done. But this whole idea of smart-pull is what this is all about. And a cloud - I want to give you a couple of definitions that I would appreciate your thinking about. Cloud is not a noun. How many of you think of the cloud as a noun? Or how many of you see it as a noun? It's just not.

Cloud computing is different from cloud storage, is different from cloud operation. So the guy I was talking about in Afghanistan, he's only interested in cloud storage. He wants to make sure that whatever the pictures that are stored there have a metadata that he can call and have it come to him. He's not going to use the cloud for processing. He can do his Photoshop on his phone. He's not going to use it for sophisticated calculations, whereas that same picture will be used by NGA with a lot of computation and a lot of operations to make a wonderful display which knows where everything is precisely and so forth. And I'm not denigrating that. I'm just saying it's a different job. So I think what you need to think about, in the cloud sense, is it's three things; all of them are 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 has to do with denying the other person the ability to work. In electronic warfare, that's called jamming. In cyber, it's called denial of service attack. They're the same thing, but the people who do it don't think the same way. And they should 'cause there's a lot to learn from both sides. There are equivalents about spoofing, influence operations, et cetera, et cetera. It's very important to think broadly about what the message is going to be and measure it against several issues. And it's very important to worry about how does the cloud processing, the cloud storage and the cloud operation interface amongst itself but then with users. Because every one of those are going to be different. And I think that the government is not good at system engineering, which is a process of taking various problems and solutions and putting them together. I used to call it having the peanut butter and jelly come out equal. And I think that that's almost definitely a failure of every government IT program. And I don't know the details of the DoD one, but I'll bet you it is not particularly well system-engineered

if you talk about it over the broad spectrum that I was just describing. So that's my context from which, if you ask me any questions, I will answer.

SCHNEIDER: This - one of the drivers for the cloud also, which Steve is likely to touch on, is the need to improve our capacity to protect information. The - as the Internet was propagated through DoD, the decentralized model of computing turned out to be - to pose a grave risk of loss of data. And, in fact, I've been a party to some discussions about is it possible for us to discuss - to conduct a war 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 been one of the important aspects of moving to the - to a cloud-based architecture. Steve?

STEPHEN BRYEN: Well, I think you're right. The security issue is certainly an issue that faces - considerably faces DoD today, and the performance has not been what we would hope it would be, hacking of DoD computers and of contractors and other people who provide support to DoD. That kind of hacking has been immense. We have seen our friends in other countries, especially Russia and China, take considerable advantage of this. The greatest example, the one that catches you most, is the compromise of the data for the F-35 program where some 50 gigabytes of information disappeared, probably to China. And it may or may not surprise you that China is now flying the J-20, their first stealth aircraft, and they're working on the second one, the J-31, which will be operational soon. So 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. Tesla, of course, makes the electric cars which we can't afford but we would like to have. And their system was actually deployed on the Amazon cloud, and it was hacked. And rather cleverly hacked, as well. And they're not alone. Other cloud systems have been hacked, too.

Now, the DoD, as I understand the procurement that we're discussing, the DoD has laid down its own standards, if you want to call them that, or guidelines, if you want to call them that, on what it expects the security of a system that it's going to procure should look like. And basically what they've done, for the most part, is two things. One, of course, is to make sure the employees that are working in the cloud environment that's being proposed are cleared American employees. That, by the way, creates a significant problem in being able to find enough cleared American employees to do the job. And I'm not sure they are so readily available. But that is definitely a challenge, let's say, that's out there. And the second is to take some of the procedures that are used to secure DoD's existing computers and servers and equipment and apply that to the cloud. So I'm just trying to wonder whether DoD has such confidence in these standards. There's not a new standard for the cloud, but they're just taking what they have and they're using a system called STIG. And I never can remember the definition of STIG so I will tell you that it stands for Security Technical Implementation Guidelines. STIG. S-T-I-G. But basically there are about 400 of these guidelines, and what they really are is massive checklists that you go through, and you're required to go through and make sure that you're in compliance with each of the points. You know, so if there's a vulnerability that's known, you're supposed to check off that and make sure that that vulnerability has been taken care of, 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 taking - a lot of them require taking down the system to fix it, and if you take down the system, you don't have it operational. So, now, how are you going to do that

in the cloud, I don't know. That's a serious, serious problem 'cause they're not going to be able to take down the cloud to fix a vulnerability.

So one of the vulnerabilities we know about these days is with some of the Intel processors that are surely used in these servers. And they have a microcode problem, and the only way you can really fix that is to shut down the system and replace that with something that's patched and works. So this is going to be a genuine challenge, but I think there's also another issue. The DoD has not been, what we could call, exceptionally successful in terms of its security. That's why it hires 12-year-olds to come in and hack away at the system, to dig out new vulnerabilities. And they're doing that right now, by the way. And it's understandable because it's a little bit of a hodgepodge system that DoD has. It's grown over the years, you know, and it's matured. And some things have not changed. For example - and it's not the most pertinent one, but it's one that gives you a sense - there are XT, if you remember the XT operating system, there are XT computers operating in nuclear submarines to this day, even though they have vast vulnerabilities. But, you know, you want to shut down the nuclear submarine and then change all the code and change all the software, it's a big undertaking so they don't do it. One of the complaints - by the way, the cloud industry is a growing industry. This year it will be about $160 billion of cloud computing in this country. That's a lot of money going into that, and because it offers efficiencies, especially for businesses - although, I must say most businesses have chosen, as Bill has said, is quite correct, have chosen to have multiple cloud providers as a way of providing some backup to any risks that they inherently have in depending on one provider.

The DoD procurement - it's a billion-dollar, proposed as a billion-dollar procurement for 10 years, but only to one provider leaves open the question, what's the backup? And that is not clear. And my guess is that the backup actually is the existing system, and that what they're really going to try to do is to keep two systems going - a cloud system over here, and the old system over here. But we already know the old system has a set of problems, and we don't know what all the problems are going to be with the new system. 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 if it was only one. So the assumption has to be that there's a backup, but the backup is just the old system that they're going to maintain. But that also sucks up the people who provide that kind of capability to DoD. Some of them are outsourced. These are cleared people. And it means as a practical matter that there's going to be not only a shortage of people, but a host of problems that are going to migrate from the existing system into the cloud itself, if they haven't already done so. So I think this whole thing is really in need of a lot more study, a lot more investigation and particularly on the security side, which I don't think is - I think what we have is a very simplistic approach to security right now that says we can put the old standards to the new system. It'll work. Everything will be fine. And I just think that's wishful thinking. And it seems to me that a much more ambitious effort should be made. 'Cause I think cloud computing makes sense, but I think that it has to, you know, it has to be secure computing.

STENBIT: I want to show that we think differently. You were talking about that funny acronym and this bunch of checklists, that you can meet all these criteria. If I were a really good attacker of the DoD cloud, I would go find the companies that are causing people to be able to check those things positively, figure out how to hack them, then I get the whole DoD right there. So it is - any checklist thing is only a guideline to your enemy about where to look. So I don't mean to be nasty.

BRYEN: No, no.

STENBIT: I am nastier than you, based on your discussions about that. And I think it's really important because you're describing security in a - I'll call it a semi-provable, insurable, kind of a way.

BRYEN: Right.

STENBIT: I assert it is impossible to secure the system. If somebody wants to get you, they will. You can do things about it. And I have all kinds of ways about how I think about that problem. But I would, just as I said you should think about cloud operations, that's really where all of this stuff he's talking about, where the programs are like cloud storage. Let's think of this simple issue. I worked on this for three years in the Pentagon. I was the assistant secretary in both Command and Control and Intelligence, and I could not get those two groups to agree on a common standard of time or place. Now, you can't have a meta-data system with a cloud storage, which everybody's going to use if you use different definitions of what time is and what location is. Some people use GPS. Some people use somebody else's standard. There's a - there's a geodesic standard, et cetera. If a user will pick one that they will stick with, it's a simple task to build a process that converts that particular position to the other one or that particular time, but they won't even do it within their own places. So I think there are, really down at the fundamental levels - I call them system engineering problems. I didn't mean to joke about them when I was talking about peanut butter and jelly, but it is true. It all has to work or else it doesn't work. And every time you start doing bureaucratic checks on that, you have provided a guide to somebody like me, to save time and get you faster.

SCHNEIDER: I think we've had a rich exposition of various dimensions of the policy issues with a decision to migrate DoD capabilities to a cloud-based architecture. But I think, perhaps, it's a good time to begin some exchange of views. And if you would, please, provide your institutional affiliation.

JOHN WEILER: John Weiler. I am executive director of the I.T. Acquisition Advisory Council. We're a do-tank made up of 24 nonprofits. We've looked at this problem with DoD. We offered to bring some solutions here from our standards partners of how do you measure this? Financial services industry, they are probably more secure than we are. The banks would be bankrupt if they implemented our checklist mentality, and I agree with you on that. But there seems to be an unwillingness to even listen to outside voices within the DDS structure. There is a closed-thinking mentality that we've already found the answer, let's back into it. It's this company, or it's this commercial cloud. Because we're so enamored with it. And we see as a greater gap, not only with the security models, that I agree with, but there is no one in place responsible that's executing on this strategy with any experience of migrating any large-scale I.T. program successfully. None. So the lack of expertise of actually doing it. I wouldn't have my brother, a dentist, operate on my brain if I had brain cancer, even though he's a good doctor and I love him and I trust him. He doesn't have the skills. He has no experience. We're doing the same thing.

SCHNEIDER: Thank you.

STENBIT: I think one of the ways to think about that is my allusion to system engineering. System engineering, a process where somebody who doesn't actually know the whole problem has a model of how to solve it, and finds experts to fix some parts of it and then works a lot about how the experts talk to

each other. That's the classic definition of system engineering. These days, it's a bunch of people checking boxes. That's not what I'm talking about. I'm talking about the Si Ramo version. But when you come with a competitive standard to me when I'm in that kind of a job, I quickly can understand whether I've already got one that I think you wouldn't beat, or I can understand that we'd better think about it. And that's what the job is of somebody who's an integrator. But the problem is that you might get an integrator of the cloud processing. You might get an integrator of the cloud storage that's probably the provider because most of that is equipment.

But, as I said, even in the storage, what are your standards for meta-data is a very important thing 'cause otherwise you can't retrieve it. And the real case is in the cloud operations. What are the programs, how do you do it? And so forth. From a security standpoint, I want to be positive about the cloud. It allows one to have the resources flexibly applied so that if you want to be more secure at a given point in time rather than some other time, like, right before you're about to invade somebody, just picture that you can, in fact, every 30 seconds of everybody in your place, switch from Linux to IOS to Windows, and you'll drive the other guys batty. You can switch from Google to whatever other search thing you're interested in, et cetera. You can change your applications because the cloud allows you to slow things down because you can add compute power, and it's seamless. I doubt anybody's thinking about the spec that goes with how do you do that with this particular system.

SCHNEIDER: The Defense Science Board did a study on security in a cloud in, I think, around 2013, and it usefully engages some of these issues. And it's on the DSB website. But these are issues that are really important, but because of the path that the government has taken where the intelligence community went wholeheartedly into a cloud monoculture and DoD seems interested in trying to replicate intelligence community experience, and there are a lot of reasons why they may not be an appropriate model for DoD and the way DoD operates because of the different missions that they have.

STENBIT: Actually, actually, I want to - I'm not sure you're right.

SCHNEIDER: OK.

STENBIT: I do know that when the intelligence community - 'cause I was involved in - went through their process. And they had parallel prototype programs, one an in-gov one that NSA did, and one a competition that the CIA ran, which Amazon won. But that's like an F-35 fighter, where Boeing builds three prototypes and Lockheed builds three prototypes, and they pick. OK? In this case, they picked both.

I think NSA's cloud is still definitely there. And if you want to do the meta-data kind of things I'm talking about, I think they're more sophisticated about it than the CIA. But I don't know that. I haven't been there for a while. However, I think that also settles a bit of your backup problem. The problem was that the people who did the joint desktop environment, which was NGA, didn't pay any attention to either NSA or the CIA's or the DoD's requirements, and so the cloud operation didn't work because it was not interoperable. It's a classic kind of a thing. You do need alternate sources. You do 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. And it's easier if you actually have - you could play games between who's actually got the baton that day. That's a whole outside the contract realm of how do I actually solve these problems? And I think that's also a very weak point of the DoD when it's basically a program element organization, and when

you need more than one program element to solve a problem or maybe three and they all have different management structures, that's a very difficult problem for the DoD to manage. And getting all their information ducks in a line is really very difficult.

SCHNEIDER: Sir in in the back?

EVENT ATTENDEE: [I'm with] SAP. I guess listening to these issues that you're raising, it prompts the question why DoD is taking the approach or is signaling the approach that it's taking. So I wonder if you could put on a different hat and answer from their perspective why would they go out understanding that these issues exist, understanding that they've got these management challenges, as well, why would they go out and create what I think many of us in the community feel is a significant vulnerability in their approach?

SCHNEIDER: Thank you.

STENBIT: I think it's always budget. I mean, the intelligence cloud was clearly there because of the squeeze in the money that occurred because of the operational issues that Bill was talking about. And somebody I know really well went someplace and said, I'll do this, and it'll save you $108.72 million per year. And I'm going to spend that. And he spent it all up - up front, and the savings didn't come. And - but that cloud, whether it's processing, operations or storage, is the sharing of resources such that you're not overloaded or under-loaded. I mean, Amazon started this whole business at a commercial level 'cause their Christmas rush was so big that their computer centers had to get so big, and they sat idle the rest of the year. And they said, hey, I'm going to marginally price this stuff. I don't mean to be too simple. But I think that's why they were out ahead. And so that's a way to say if you don't have a constant information load, you can save money by sharing. So let's say you're doing a biochemical modeling of DNA, so you can do some sort of really monoclonal antibody. It takes an enormous amount of compute power for a very short period of time. The cloud allows you to sign up for that enormous amount of compute power. And then five seconds after you're finished, you turn it off and don't pay any more. So I think it's always money. But after that, somebody's got to worry about what it does.

SCHNEIDER: Just on the point relating to funding, General Clapper, who was the DNI at the time, specifically expressed the view that the intelligence community could save about 50 percent of its IT budget by going to the cloud. And they were looking at this very steep ramp for costs if they didn't do something like that. So it's - if you're driven by circumstances, as John suggested, to focus on budget, you want to believe.

BRYEN: So I just think that they haven't paid nearly the attention they should be paying to security. And this is a decision that looks just like that. I mean, DoD has constantly bought IT, IT, IT and then scrambled later on to try and fix what it bought. You know, you have a place across the river there that is 80 percent full with computers made in China. So you can figure out the rest.

SCHNEIDER: In the back.

EVENT ATTENDEE: [I'm with] a small company called YottaStor. I have a lot of stuff to say, but I'll keep it short. First of all, six years into the eyesight experience, none of those value propositions have been achieved. And now Azure is being brought in as a competitor. What's interesting in that space is

maybe there's been success on the CIA side of using the cloud. But the four DoD intel organizations have struggled mightily to have that support their workload. And it seems like those lessons are being lost on OSD proper. On the security side, given our new national security strategy and the near-peer issue with China and the fact that to run commercial cloud in China now they have to be run by Chinese organizations - that's almost a zero-day exploit parade ground for the PLA to understand how to get into Amazon now in the commercial space. And there's nothing in the OSD security RFI that talked about how you're going to firewall off that knowledge. So it seems like, you know, the lessons that we've learned - six years and billions of dollars - in the new world of cloud are just not even going to impact the OSD organization. I'm wondering how that can be and what all your thoughts are.

BRYEN: You can see they just imported the procedures they already have. Not - nothing new. I mean, just the system that they have they're applying to the cloud. So they don't even have a STIG - excuse the phrase - they don't even have a STIG that really is addressing cloud issues, which have a lot of management systems that don't exist in DoD systems. So I - you know, you have made it very clear, I think, about what the situation is. It's really trying to comprehend why it's like that. It's troublesome.

SCHNEIDER: I think there are a lot of industry lessons learned that might be exploited with benefit to the Department of Defense, saying - noting commercial practice, where they can have the convenience of a single provider or the complexity of managing multiple providers - is that because the industry is quite vibrant and has produced many alternative ways of delivering these services based on the needs of the user - that 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, where new providers may have different ideas about whether it's relating to security or process efficiency or other merits that can be attributed to cloud-based architecture. I think 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 the cloud services.

STENBIT: I think it's a fundamental problem. I've been in OSD twice. There's a Secretary of Defense who, in theory, manages three services and some agencies. He doesn't have any money. All the money gets appropriated to the services and the agencies. That's not quite true. I mean, he has a little bit but not a lot. And he has a "staff," quote, unquote, to pull the peanut butter and jelly together. That staff has gone through all kinds of reorganizations in the past. But fundamentally, it operates on program elements. So it's a way to manage program elements, whether they're R&D or procurement or O&M or personnel. And various people have jobs like that. The problem is information. You mentioned the F-35 and how dependent it is on information. I was there, and I said, my God, the F-35 has the best radar around. I want to get the radar data back out of that thing because that's going to be better than a lot of other things we have, including very sophisticated systems that people love. And of course, the guy that runs the F-35 program says, you got to be kidding. You're going to blow my stealth. And we had some fights about the other ways I could blow his stealth, but that's a different issue.

(LAUGHTER)

STENBIT: However, information is a parallel issue that doesn't follow a program element. And so there's an undersecretary for intel. There's a CIO. When I was there, there was a - I was ASD of C-cubed and I. That was a reasonably good combination, and I was the CIO. But I always let the finance guys worry

about the business stuff because I didn't - I mean, that was a much different issue. You can't have a secretary and a deputy secretary who are very busy who have to integrate what the intel guy says, the CIO guy says, the procurement and R&D guys say on an information basis because he'd be sitting there all day long, being a system engineer. And there is no such person. So information is fundamentally a - it shouldn't be split. That the maximum number of organizations responsible for engineering - information in OSD is the wrong solution, OK? I quit when Mr. Rumsfeld did that - split what I was doing apart because I said to him you need to find someone who actually believes that's the right way to manage this thing. So - but what you're talking about is - that's not going to get fixed.

SCHNEIDER: This is - you know, again suggests perhaps an alternative acquisition model, where some of these issues can be identified and worked out before it's propagated. And for that, the opportunity to take advantage of the vibrancy of the industry, the rapid technological change that's taking place and the enabling technologies that support cloud-based IT seem to be a way of reducing the risk that DoD undertakes by having a highly centralized platform for its storage processing and operations.

BRYEN: You also have to make sure that understanding - the level of understanding of the system outside of the United States is low because, I mean, one of the things that concerns me is that the architecture of these systems is not confined to our borders and that the supply chain that supports it is all over the place but also mostly in Asia. And we're - our friends in China have supercomputers now that are outperforming the supercomputers that we even have. So I think we're setting ourselves up for a lot of trouble by migrating to a kind of generic system without studying. I'm not saying we shouldn't, but I'm saying we should study the implications because we know very well the Chinese are not only extraordinarily active in this field. They're also good at it, and they're also requiring cloud providers to not only provide all the information about their systems. But also, the encryption keys that they have must be shared with the Chinese in order for them to operate, you know, with Chinese entities and Chinese companies. So I think there's a lot of risks here that - I don't see any assessment. What really bothers me is that this whole thing is just really looking like kind of standard procurement with all these unsettled issues swarming underneath. And no one's paying attention, and that's scary.

STENBIT: I think it's too pessimistic to say that this can't be done, but somebody has to decide they want to do it. We used to design really high-quality systems out of parts that weren't very high quality. And that's an engineering process where you have to be able to work through that process. In security - and I think that's a big deal here - but I'm not at all against DoD worrying very hard about cloud processing and cloud storage. I believe there's a lot of money to be made there, and there's a lot of good things that can happen. It can also get fouled up if you don't get the metadata right - all that kind of stuff. But I think that having a great, general-purpose set of instructions set isn't going to help a guy who's got a complex radar that needs to do radar processing. And they're now trying to get radar guys to use the cloud instead of radar processors because that's the way they think. That's - those are the kind of errors that are made. The security issue I look at very differently, I think.

There is no way to be secure. I absolutely assure you there is no way to be secure. If it's not too hard, you can do the bear in the woods thing. You don't have to beat the bear. You have to beat the guy that's running with you. Well, that's not funny. It's a perfectly valid thing to do is you'll get the hackers to go after the other guy if he's easy - easier. That doesn't solve the real problem in my world. I think you have to have a five-layer system. And because the amount of effort that goes into it goes up a lot, the more

secure you want to do because you want people to continuously attack you that are your friends. You want to monitor very closely what everybody's doing, almost bit by bit, to see if you've got an internal guy who's already bad. You start with a kernel. And I would call that the first level of the operation of the cloud – of all three. And if you want to think of it in intel terms, it's just the overlay that gets started with the information. And then you're going to go to the TS/SCI kind of level. There's a boundary. You're going to watch every bit that goes through that boundary. You're going to fondle it. You're going to make sure it's the right one because you can't afford to have bits go across that boundary and get to - in a computer, the equivalent of a BIOS.

You know, I get things to change my BIOS on my computer all the time. And every time it happens, I say, OK, this is giving away the store because I don't know what they're doing. Hope they're the right guys. You can run a pretty good enclave of pretty secret people. Both the DoD and the intel community know how to do that in - where they have some freedom of what the processes are. If they get forced into a generic cloud, they'll have a harder problem solving that. But just think about it as, OK, then I need to go to the third layer which I'll call secret or that kind of stuff. And there's - got to have a lot more access. You can't monitor every piece of data. You can make sure that you don't go from the TS/SCI one to the secret one unless somebody is really paying attention. And you can have ways that you filter what you're interested in coming the other way. But that's a different management problem at that level. And then you can go to whatever you want to call it - a little bit classified. And then finally, you go to the Wild West. You have to be able to do the Wild West. You'd apply a totally different set of security context. I think you can't - I mean, the cloud is a part - cloud processing - cloud is a part of the whole of DoD. So you have to have some mentality about this layered thing.

You have to, absolutely have to dynamically assume that you have already been had and search diligently. I find how difficult this is commercially. A friend of mine, very involved with a company that if you pay them will tell you how many Russians, Iranians, Chinese, et cetera have been in your network over the last six months. And they go to places like Goldman Sachs and Bank of America and tell the CIO, you know, there's currently 92 people from Russia in your stuff, 87 from China and so forth and so on. And the CIO says go away because the CIO has told the CEO that everything's safe and he's been doing a good job for 10 years. And they actually don't accept the data because it screws up the - I didn't mean to imply that Goldman Sachs or somebody was civic about that. I was making a general comment, OK. Well, I'm a little sensitive, but I'm using an example. That's what happens. So you have to get through that. And you have to be happy when somebody says, boy, those guys are there. Then you can decide whether you're going to let them stay there and watch what they do because you'll learn a lot more about what they're doing if you let them stay there and watch them. That means you have to set up a honeypot and a whole bunch of other issues. I don't want to go into all of that. But somebody's got to worry about that or it won't work.

EVENT ATTENDEE: Oh. OK. The gentlemen bring up great points again. One of the things I keep asking myself and others is we just awarded milCloud 2.0. If we're not happy with it, why not fix it? Because you have an organization set up to manage that. You have, like NSA, a protected enclave, like CIA, that's not a public cloud. So we really have not proven that a commercial public cloud is even secure enough for us. Why are we not taking advantage of the investments we just finished making? And I don't understand the politics behind ‘let's ignore what DISA just did’. Is it ego among the folks running this

procurement because they want to say they succeeded in bringing government to the cloud, which we're already in? We have 500 different cloud implementations in DoD already. Thank you.

STENBIT: I don't know what that program is, so that's easy - don't worry. They'll tell me. I just - I can't answer anything. So yeah.

SCHNEIDER: I think we had a question here.

EVENT ATTENDEE: I'm with Open Markets Institute. How does the PLA handle this problem?

SCHNEIDER: Well, they keep a lot of their stuff out of - off the Internet. They have a dedicated strategic support force. That's so that you don't have the capabilities spread out all over their military forces. Their civil networks are much less accessible than has been the case with commercial networks outside of the government. So I think that they have undertaken a layer of protections that's - for a variety of reasons, not only military that make their system a lot tighter than ours. In fact, in most of - most modern countries who have a much more relaxed view of the role of the Internet, the role of networked computers and the way in which storage will be undertaken. They do have also a vibrant industry that is providing and will continue to provide cloud-based services as well.

BRYEN: And they're also working on their own operating systems instead of using commercial off-the-shelf ones as a way of making it more difficult for hackers to hit them. I think that's a very interesting development on their side. And I think you have to add that they're not nearly at the same level as the American defense system in terms of the level of integration of services and capabilities, nor are the Russians. They're very far behind us. In fact, you know, part of this whole revolution in military affairs and the qualitative edge that it has provided us, as Bill started talking about at the beginning, has been really one of our greatest assets in terms of force multiplier and in terms of the capabilities that we're able to get. And frankly, when we were struggling against the Soviet Union, that was how we beat them by having these kinds of electronic capabilities they simply couldn't duplicate. They couldn't get near it. And I don't think they're near it yet. So - which also creates an asymmetry in the sense that we have this vulnerability because the more computing that we rely on, the more satellites we rely on, the more fiber we rely on, all these things can be attacked. And that's exactly what's happening.

STENBIT: I think I would rather be on my side. They have a lot more people. That's an important thing. They really have a lot more people doing information operations just because they have a lot more people period. And they're well-trained. But hierarchical-controlled societies - and I'll go back to the Russians when they were 10 feet tall and all the rest of that, and my job was to make sure they weren't 10 feet tall - they're amazingly easy to blow apart once you get through and find some vulnerability. And they're there because they're afraid to test things and so forth and so on. The Chinese have a very robust industry, but they won't allow their own people to have a lot of information. So there's a lot of hierarchical problems. I mean, here I'm talking the whole day about I want the Internet to get the right data to the right person whenever they want it and they get to choose what it is. Let me assure you, neither the PLA nor the Russian military is at all interested in a fighter pilot being able to get any information he wants because they're very afraid he'll turn around and go to Moscow or Beijing.

SCHNEIDER: This does raise a dimension of the cloud-based architecture which relates to the question of how we work with our allies. We - our allies are going to be increasingly important players in how we conduct warfare. The F-35 aircraft is being sold to European, Middle Eastern and East Asian allies. And somehow, if we're going to inter-operate, whether it's with tactical aircraft or the more recent decisions made to have U.S., Japanese and South Korean missile defense collaboration where we will need to be able to have this data integrated and operated in near real time because that's the nature of the missile defense problem. We need to be thinking about how to manage this sort of data in ways that contribute to the security of our allied partners as well. I think we have the discouraging example of the Libya campaign, where the U.S. made a decision not to lead in the campaign. And that produced a lot of unhelpful outcomes because of the inability of the allies to share data and to use it in constructive ways. So I think 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 the military aims of the alliance and to do so in a way that's as efficient as possible. You know, we're not there yet.

STENBIT: That reminds me. I was sent to Kosovo - no, sorry, Bosnia to check up that the Russians had gotten the best of our satellite imagery that we gave them when they were our allies. I found it a very frightening kind of a thing, but fortunately, it was another contractor who had provided the equipment. And I felt very good about that. However, it turns out we went and visited the French. They were much more aggressive and ruthless about what they were doing in intelligence use of what we were doing as opposed to using the pictures in the first place, than the Russians. So I think you need to understand that who's a friend and who's an enemy is not a constant. And those are going to be real live things. And so as I say, you've got to be dynamic. And you've got to be checking all the time. Then you can decide whether I'm going to allow this or not allow this or whatever.

EVENT ATTENDEE: Hi….I'm a researcher here at Hudson. You've highlighted a number of issues with the DoD procurement of cloud computing services. Do you think those issues will be exacerbated by kind of a single award IDIQ contract as opposed to a multi-cloud solution?

STENBIT: Doing system engineering on a multi-cloud solution is harder than it is to actually do reasonable trade-offs between the DoD and a single cloud because there's only one guy you have to fight with. So I think there's always an advantage to having multiple things as long as they're bringing different issues. The point of saving money is you combine it. That's, I think, is going to always drive it to one. And if you're going to decide that there's a reason to have two, then you better understand that you've actually fixed the whole problem. Otherwise, you're going to have two of the whole problems and they're going to be different.

BRYEN: But the private sector use of cloud - usually in multiple providers. And so why is that? Is it for budget reasons, or is it because reliability, availability, stability and dealing with problems? And one of the things that's reported very widely in the cloud sector is there are problems. There are problems between the IT people and the security people. There's problems between the companies and the provider. And it goes on. And a lot of these are still really unexplored. So I think there's a - I don't know if I'm taking issue with you or not. I really don't think so. But I think that if the general trend is to have multiple providers, then one has to think it's not just for money but that it's a pragmatic and operational decision that makes the most sense.

STENBIT: OK. If I'm a drug company and I want to do molecular modeling or DNA modeling in order to come up with monoclonal antibodies, and I have five clouds that I can use, I'll use all five of them because I've got five of those projects. I mean, that's a different problem from waging a killing war.

BRYEN: Well, I'm not sure it is. I mean, that's an interesting issue because it seems to me that you don't want one vulnerability in a war because then you might pay greatly for it.

SCHNEIDER: Yes, sir?

UNIDENTIFIED MAN: I have to say this is a very frustrating discussion because there are so many questions and politeness requires us to pick one. So I guess, you know, we've had this - there's always this tension between commercial and proprietary or privately developed, government, unique, whatever we want to call it. And we're relying here heavily on commercial. We're saying, let's leverage the commercial space. The JEDI document speaks to utilizing a commercial-level security. And, you know, so of course you have this threshold question of, what is that? And is it better than the security we have? Are the assumptions sets just - have they been tested yet for this approach? Because it seems like we're moving forward. And I guess the implication of the answer is to what extent is there a value add by DDS in this process because there's a quandary here in the industry as to how they're laying out their requirements here. What's justifying - where's the data, if you will, to justify this approach? And we're not really getting an answer.

SCHNEIDER: This issue has come up in the omnibus appropriations cycle. And I think it's been surfaced. And so I think there's some likelihood that Congress may choose to get involved in this in some way. And Congress has been the big driver in - you know, competition, Contracting Act and lots of activities of that sort to try and maintain them with the presumption of competition in DoD procurements. And the service industries have generally been better served by the competitive procurement than the procurement of hardware simply because the industry has tended to be quite vibrant - large numbers of participants in the market. And hence, it's been easier to run competitive procurements for them. My concern I had, which I mentioned at the outset but I think is worth raising here, is that the DoD process needs take advantage of the dynamism of the industry. These are technology driven - it is a technology-driven industry. There's many dimensions to this that are being altered, enabled, et cetera. And not all of the same services are going to be offered by every cloud service provider. And so the DoD, in an effort to maintain a posture of continuous innovation, needs to find a way to manage that. And a single service provider may not necessarily be the way to do that, or else there needs to be some contract innovation. That has not been one of DoD's strong points. Yeah.

BRYEN: (Laughter).

SCHNEIDER: Yeah, it's...

STENBIT: Well, look, DoD's procurement thing started back after World War II. And ultimately the Packard Commission in 1970 came up with the organization that is there now, and it deals with program elements. I've said that several times. And the problem is when that one - more than one program element is needed to solve a problem, and that's when the problem occurs. The issue is that without somebody owning the output as opposed to the input - there was a lot of work done on OT&E to make sure that you

couldn't get your money until the thing passed. That would be an answer to your question, which is, what's the TEMP? What does the TEMP say? That's the Technical Evaluation Management Plan, I think is the name for it.

BRYEN: Right.

STENBIT: But it's basically the final test of whether you get paid or not. If somebody were to really rigorously define the use cases that you want the TEMP to pass, you would discover - as opposed to arguing about adjectives in piles of paper that are this high called an RFP - it would be a lot easier. And a lot of people would lose money because they're not used to it. And the real issue is you keep the bureaucrats from changing anything 'cause once the TEMP is written, they're going to pay. And it can't - and whether it's your constituent or whether it's your office versus somebody else's, all of that sort of goes away. So as long as you're worried about inputs and measuring of inputs - and that comes from Congress. They want to know that the color of money is kept pure, and they don't actually care what happens. It comes out the other end. They care about what the feedback from their constituents is but not in a technical sense. If you worry about the output - you know, does the plane fly? Does it - you know, does it meet stealth and all the rest of those things? Then you can have an argument about whether you want to buy them or not or how many or whether you want to fix them. In IT, we don't do that, and yet we should. And we should have a hacker go after it. And you'll discover that nobody will ever get paid.

BRYEN: (Laughter).

STENBIT: No, I don't mean to be cynical. But I mean, there are simple rules that people need to follow. And I actually don't know the details of who DSS is or what they're doing. But the idea that it's a committee or OIPT or whatever they call them these days - it's going to go through all of that. That's not a way to procure an IT system. That's going to have pressure on it from operational difficulties, security difficulties, people shooting at it, et cetera.

SCHNEIDER: Well, I think this is an area that's been moving along for several years without DoD really engaging. And the engagement appears to be sort of binary - that they have gone from, say, monitoring the IC's progress with it and thinking about it to a decision that - are going to go quickly. I think it was - at least an important part of it was related to security, as I mentioned at the outset, that the present system is definitely not secure. And well, I think people close to (unintelligible) share John's observation that it can never be secure in the sense that it's airtight. You can just...

STENBIT: You have to manage security.

SCHNEIDER: ...Manage - yeah - manage the risk in such a way that you are able to conduct operations with a fairly high degree of confidence that you'll be able to mitigate the opportunities for the bad guys to interfere, recognizing that at some - in some circumstances, they almost certainly will be able to disrupt elements of our operations. But the DoD has elected to move very quickly. 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's, of course, a potential risk here as to recovery from a bad outcome. You know, what are alternative acquisition models that might be undertaken to facilitate a recovery? As I said, they'll be a - if they move

quickly they - some of the mistakes that John and Steve have pointed to are likely to appear quickly. And that is a source of concern. So we have about 10 minutes left.

STENBIT: I think - maybe I can comment. I think it's worse now because, I think recently, they took the procurement away - procurement authority away from the CIO, which used to be able to use Clinger-Cohen, which is a totally different model for - and it's actually useful for some of the cloud kind of things we're talking about. It basically says if you can define it as a fixed-price contract, you don't have to go through all that stuff. So now, DDR&E or whoever's in AT&L, who really is totally managed by program elements, is the guy that decides who wins. And so, I mean, there are some real, real impediments to doing this correctly. I'm sorry. I interrupted one of you.

SCHNEIDER: Sir.

EVENT ATTENDEE: Thank you. [I'm with] the firm Luks Cormaney. Question - I used to work for somebody that very few people remember, Abe Ribicoff.

SCHNEIDER: Yeah.

EVENT ATTENDEE: OK. Ribicoff always used to say, organization is policy. Sometimes yes, sometimes no. So here's the question - if you look at the current structure leading toward the expected procurement, which we're discussing now, what specific changes would you suggest in the organization to try to expand and address the multiplicity of questions and issues that have been raised today? And a subset of that is - should there be people involved from other agencies outside the DoD community?

SCHNEIDER: Well, thank you. It's a good question. I think that because of the nature of this, the DoD has created an ad hoc mechanism to facilitate the rapid procurement. And that has a lot of positive features in that it focuses the 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 that get it raised here and, you know, hence contributes to the risks that you won't have the outcome that DoD both needs and seeks.

EVENT ATTENDEE: And the oversight.

SCHNEIDER: Right. Because it is an ad hoc arrangement to meet this particular need, the oversight arrangements will have to mutate the existing institutional oversight in order to manage it. But as far as I know, that has not been specified.

BRYEN: It wouldn't be a bad idea to have the Defense Science Board review this whole procurement.

EVENT ATTENDEE: Absolutely.

BRYEN: I think that that exists. They're from industry, for the most part, and from the private sector.

SCHNEIDER: They're not procurement.

BRYEN: They're independent of the system. They think well.

SCHNEIDER: Yeah we're - the DSP has in its charter - it's specifically prohibited from reviewing so-called particular matters, which - I'm not a lawyer, but...

BRYEN: Is this a particular matter?

SCHNEIDER: ...If you're on the wrong side of it, you get to wear orange. And I think that...

EVENT ATTENDEE: Congressional research service or GAO, I mean, they could look at this.

SCHNEIDER: Well GAO - no doubt GAO will...

BRYEN: Will look at it anyway, yeah.

SCHNEIDER: But this is a - it's really a procurement policy - or acquisition policy matter. And it's - it doesn't quite drop into the box associated with science which is more about technical choices. And the congressional oversight agencies will look at aspects of it but it probably will be difficult for them to surface the issues that are needed. And usually they arrive after the train wreck...

BRYEN: Right, right.

SCHNEIDER: ...Rather than before.

STENBIT: It has to be ad hoc. I mean, if the organization doesn't match what you're trying to do, it has to have an ad hoc mechanism. And then somebody has to either be given or take the power to be responsible. And it's usually somebody that takes it. Certainly, when I was around, I was the one that took it. And Mr. Rumsfeld would say, what are you doing? And I'd say, I'm doing this. And this is what's going to happen. And if it's going wrong, I'll tell you. And I set up my own ad hoc set of things, which was most - we deployed, for instance, a commercial-grade, fiber optic network around the world for DoD use to enhance all of this stuff – fixed-price, on-time. But I had the J6 of the JCS in my office two times a week. And I'd say, hey, you guys you said you - that Guantanamo was one of your high-priority places. I said, OK, we're fixed-price. That's out of the way. We got to run fiber. Which of the - would you like to get rid - of Syncpat or Synclant or maybe Syncure, or would you like to go to Guantanamo? And she came back the next day. She says, I think we won't go to Guantanamo, but somebody has to do that. And I believe there's an ad hoc organization that has a committee running it. Is that not true? Doesn't DSS have...

SCHNEIDER: Right.

SCHNEIDER: Yeah. Well, DoD has - has shown itself to be pretty good at implementing ad hoc arrangements. The mine-resistant, armor-protected vehicles were put - we built 12,000 of them in three years. And for most conventional procurements, you can't get a dial tone in three years. So DoD is quite good at executing ad hoc arrangements. It's just that this - the technology doesn't reside in the DoD. So the DoD is not, in that sense, intimate with the technology the way it might be of a specialized defense.

STENBIT: But General Meigs did the right thing. He set up a very ruthless...

SCHNEIDER: Right.

STENBIT: ...Set of people to help him do his ad hoc thing.

SCHNEIDER: Right.

BRYEN: And it seemed present right now. I mean, it seems like this - the security side of this, which is what I know more about than the other, just doesn't seem to be addressed in a serious way. And I think that's...

STENBIT: That's because C-Cubed and the CIO are IT, and cyber security is intel.

BRYEN: Yeah, I understand that. I understand the institutional problem.

STENBIT: So the secretary is the integrator. Good luck.

BRYEN: Well, maybe he needs good luck...

SCHNEIDER: Yeah.

BRYEN: ...Because this is something that this gap has to be bridged. And whether it's an ad hoc group, or whether you use CYBERCOM, or you use NSA - you use the assets you have. But you have to look at it. And I don't see where it's looked at.

SCHNEIDER: Yeah.

STENBIT: NSA is not a paragon of procurement.

BRYEN: (Laughter).

BRYEN: I'm not talking about procurement. I'm talking about risks.

BRYEN: Exactly.

WEILER: John Weiler again. One thing that I keep asking myself is, what problem is the part we're trying to solve? And that's not been succinctly articulated. Not having an enterprise cloud solution is not a problem statement. Not being on the cloud is not a problem statement. You know, the fact is that many of the problems that we're seeing is because of how Congress funds programs. If there's no funding for ubiquitous IT infrastructure, there's nothing funding the fact that we're going to create capabilities that are utility computes for all programs. Each program is funded a specific color of money. But we haven't seen...

STENBIT: No, no, no. That's not true.

WEILER: We haven't seen that done well. I mean, this...

STENBIT: No, no, no, no, no, no. There are lots of defense, industrial-funded IT programs.

WEILER: That are just infrastructure, separate from the applications?

STENBIT: Absolutely.

WEILER: But maybe that's the problem - that it's not been well done.

STENBIT: Well, I disagree with you.

WEILER: OK.

STENBIT: I'm sure there are some that aren't well done, but I know several that really work well.

WEILER: OK.

EVENT ATTENDEE: We believe, from our perspective, the communication model is it goes from the top federal executives - CIO, CTO - that goes through the cloud - providers, people that work at the cloud providers. And that information is pooled. And it goes into JEDI and other - they're experiences. That's what's happening. We know this for a fact. So if you're concerned about, no one knows about this or the economies - I'll say economy is a scale, then the information created from the economy is a scale. That experience - all that knowledge is kind of hidden. It's kind of in the back room, but it's definitely getting to the right people. And take a look at what's not in the procurement. Look at how it's written. There's a lot of things that aren't there. And look at what was said. Bring your A-game. If you have an answer - if you think you have better answers, or you see something from a Six Sigma model that isn't defined - you know, this week - the week of the ninth - is when the answers are supposed to come back. We're not even there yet. They're saying, we need to move fast on this. We need input from the industry. Bring your A-game, and bring all these ideas and present it in a formal response. Thank you.

SCHNEIDER: Thank you. Well, this is the first meeting we've held on this. And the aspiration, of course, was to surface the issue and not try to resolve them because undoubtedly - as DoD moves into this acquisition - there'll be more clarity as to what outcomes DoD is seeking and how they intend to deal with it. And we can revisit the matter in due course. So...

SCHNEIDER: Thank you, or - good. Any last parting...

STENBIT: Thank you.

SCHNEIDER: ...words? Well, that's...

BRYEN: Good dialogue. Thanks.

SCHNEIDER: Yeah. Good. Well, thank you for participating - very helpful.

(APPLAUSE)