Hudson Institute

Lessons Emerging from the JEDI Cloud: Immediate Steps and the Future of Next-Generation IT

- William Schneider, *Senior Fellow, Hudson Institute*
- John Stenbit, *Former Assistant Secretary of Defense for Command, Control, Communications and Intelligence, U.S. Department of Defense*
- Fred Schneider, *Samuel B. Eckert Professor of Computer Science, Cornell University*
- Tod Lindberg, *Senior Fellow, Hudson Institute*

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
September 14th, 2018

TRANSCRIPT

Please note: This transcript is based off a recording and mistranslations may appear in text. The names of participants in the Audience Q&A have been removed. A video of the event is available: https://www.hudson.org/events/1596-lessons-emerging-from-the-jedi-cloud-immediate-steps-and-the-future-of-next-generation-it92018

TOD LINDBERG: I'm Tod Lindberg. I'm a senior fellow here and am joined by an exceptional panel to discuss the issue, Lessons Emerging from the JEDI Cloud, Immediate Steps and the Future of Next Generation IT at the Department of Defense (DoD). So let me introduce the panel briefly, and then we'll get into the session. I should mention that we'll be ending at 10:45 today. One of our panelists wants to get on an airplane before the storm descends upon Washington and I think that's a prudent consideration. So, with your indulgence, first let me introduce Bill Schneider, who's a senior fellow here at the Hudson Institute and is heading up our effort that's looking into this set of public policy issues surrounding the Joint Enterprise Defense Infrastructure (JEDI) procurement and other related matters of IT at the Pentagon. Let me also introduce Fred Schneider – no relation, I should say, to Bill, or so I'm informed. Fred is the Samuel B. Eckert professor of computer science at Cornell University and also chair of the department there. He's done extensive work on cybersecurity issues and has been active in a number of academic and consulting aspects related to those questions. And then there's John Stenbit. John is former assistant secretary of defense for Command, Control, Communication and Intelligence, C3I, if I have that right.

JOHN STENBIT: Correct.

LINDBERG: OK. It's not always an easy thing to get the acronyms right. I may have to interrupt our panel from time to time if they resort to abbreviations and acronyms in discussing this subject and ask them to clarify. John's also been a member of the Defense Science Board, the National Security Agency Advisory Board and additional advisory boards, so at a fairly high level of technical expertise in strategic consideration. So with that in mind, I will take a seat. And I'll ask Bill to begin, maybe by catching us up with where we are in the process with regard to the JEDI procurement. Obviously, there's an RFP out, or request for proposal. And Bill, why don't you just take it from there and catch us up on that?

WILLIAM SCHNEIDER: Sure. Well, as many of you are probably already aware, DoD has been in pursuit of creating this JEDI program for several months. They've had a few initiatives to reorganize the management of the contract and so forth, but the bids are now to be in early next month. And my understanding is that DoD is finished with tweaks to the RFP, so it's likely that the contract is likely to take place. There's still quite a few uncertainties from the perspective of an outside observer about exactly how the various awards are going to be evaluated, although DoD undoubtedly has the criteria they have in mind. We've had some commentary about the question of a roadmap. It's usually the case in the way DoD operates for significant procurements, is that they have a roadmap that indicates the long-term plan. And they have produced one, but it has not yet been published. So it's difficult to comment on it, but it's clear that cloud-based IT architectures are going to be a central part of how DoD conducts its operations and supports U.S. military forces. So I think we're, for better or worse, well-advanced in this project, and it's likely to be initiated. Whether it's going to be able to work around the problems of legal challenges to the acquisition, which has often been a problem with service contracts, remains to be seen. But DoD is clearly very committed to this program, and I think it is likely to have the initial round of decisions made next month.

LINDBERG: OK. Thanks very much. And let me now turn briefly to Fred and ask: why move to the cloud? What is the objective here, and what happens once a contract is set?

FRED SCHNEIDER: A good starting point for why move to the cloud is, roughly speaking, "What is the cloud?" Commercial cloud providers offer collections of machine rooms. Each machine room has lots of computers and storage devices in it. And the result is, because these resources are shared among a large number of customers, they can provide not only access to shared processing and data, but the access can be elastic, which means when you need it, there's likely to be the capacity for you to have it. It means that you can do sharing between applications that might not be likely to share because they're not co-resident. And it means that somebody else is managing the hardware and probably the software, which means you don't have to do that. Because the machines rooms are geo-distributed, it means that there's some measure of reliability because physical events tend to be geographically local.

So then why does it make sense for DoD to move there or for DoD applications to move there? For one thing, the rest of industry is moving there. And that means large investments are being made in developing applications and services. We could take advantage of that within DoD if we run them on the cloud. It also would enable DoD to take advantage of two new trends. One is so-called big data and the other is machine-learning, where one uses automated methods to analyze and make inferences. If DoD doesn't position itself onto a platform where these kinds of things are available, then people won't be able to experiment, because the data won't be there and the computing capabilities won't be there. There are likely fewer configuration vulnerabilities if DoD moves to the cloud, because fewer people are managing each machine room, and they're likely to be more skilled and more attentive. Cloud providers tend to be more attentive to security updates and so on. The stories of running very outdated versions of the operating system are not stories that you will find in a cloud.

On the other hand, a cloud would tend to be a monoculture. That is, the way to get this scale is by replicating hardware and replicating software. That means if there's a problem with one, there's a problem with all. And that makes clouds attractive

targets or attractive nuisances. And if you're worried about exploiting supply chain vulnerabilities, then knowledge that DoD were using a specific cloud would tell our adversaries what kinds of hardware DoD is using, and that might allow somebody to try to leverage a supply chain attack. If you look at what's happening commercially, because of the last three years' widely publicized attacks, the various cloud providers, many of whom try to work internationally, have started to make big investments in making their clouds secure, because they're worried about their foreign customers not being willing to do business with them. And the result is the desires and targets of commercial cloud providers are very well-aligned with the idea of providing security for their customers, even if the customer is DoD. And that means DoD gets to ride a trend. That is surprising. Usually, DoD has security concerns that are independent.

LINDBERG: Thanks, Fred. John, talk about this. Tell us about the scale of this procurement and how that compares to previous undertakings of DoD.

STENBIT: Traditionally, DoD IT budget writ large, if you want to put in communications infrastructure and things like that, has been about 3 or 4 percent. That would be these days – I got to answer – $20 billion, or something like that, per year. I'm not saying it's the same today but just as a number. I think it's gone up and it's gone down. And that's a big number. The problem is usually couched, in addition to what Fred talked about, as we can save money, because this is a shared system, and not everybody is wasting all of their cycles on the desktop when they're not there, etc., etc. We used to have a really, very secure IT system that was well-integrated and had a lot of security and a lot of control, and it was centrally controlled. It was called a mainframe. So when I was growing up, if you programmed a computer, you got a bunch of IBM cards. And you handed to some guy who put it in the machine. And the next thing you knew, you went down to the other end, and you got this stack of paper, which was green and white-striped. And it had holes, and it came off of a reader. Now, those were actually quite secure. They were very efficient at using a very scarce commodity, and the users hated them.

OK. And now, what is an environment that went from that, to minicomputers, to client server, to what is today an all-out-free-for-all in terms of desktop capacity, internet, I can go share with anybody, etc., etc., etc.? Very vulnerable to everything that Fred talked about: disruption, security. Cybersecurity is an issue of the weakest link in the network, and so there are a lot of opportunities in the current environment for bad things to happen. Part of the issue of the cloud is to get back to the logical equivalent of the control that existed in the old days. And the reaction to that is going to be just the same as, "I will predict the reaction to that is, and the users will hate it," because the succession of implementation of control will cause not to be able to do things that they were used to doing. So I believe, first of all, the money is so profoundly possible. If it's really $20 billion a year and we can save $3 or $4 billion a year of real money on real stuff and still have the same number of storage bits and compute power and so forth and so on, that's real money in a real world. And who was it that said – Dirksen?

LINDBERG: Yeah.

STENBIT: "...A billion here and a billion there. And after a while, you got real money."

LINDBERG: It's real money. Yeah.

STENBIT: So I think there's an imperative for this. I worry, given the distributed power in DoD, that the money guys tend to win these jobs, these debates, when the techie guys get a little bit loose. I'm sorry if I tell you stories, but I'm trying to tell you the real life. When I went into the Pentagon at 9/11 time and we were attempting to move everybody towards an internet system where we were much more flexible about getting information to people and so forth, we built a dedicated fiber network for DoD, which we did the right things to make it redundant, made it secure, made it very much more difficult to penetrate, tested for penetration and all those kind of things. And it was done so that we could rapidly align data from – let me call it – STRATCOM to EUCOM, if, in fact, there were a problem in the Baltics, and we needed B-52s that STRATCOM control to get over there and that they could actually interact between the command centers with very wideband systems with lots of good photos and all the rest of the good stuff. What did PA&E the day I left the Pentagon?

LINDBERG: PA&E is...

STENBIT: PA&E, excuse me. It's not even what it's called anymore.

LINDBERG: Yeah, it's now called...

STENBIT: But they're the money hounds in the Pentagon. It's what Alain Enthoven made his fame with Secretary McNamara about. They told all DoD people they had to use this fiber optic for their commercial communications so they could stop paying Verizon for their phone bills, so they could save whatever it was. Absolutely the wrong use of a command and control system. But that's what happens when you build a system of some complexity with flexible opportunities. So my issue here is, I think it's good to go to the cloud. I would tend to believe you should think about cloud storage independently of cloud

processing, because what you do with the two are different, and the implications are different. There's money to be saved. There's opportunities for better interoperability.

But, to give you an example, when I was trying to make this internet center thing go, there are two pretty critical numbers in an intel system or a DoD system: position and time. And DoD and the intel community could not agree on a common standard of how to measure time or measure position. Now, it turns out all the interoperability in the world is useless if you're using Greenwich Mean Time and I'm using Naval Observatory time. There's a lot of money being made in Wall Street trying to shrink the time delay between somebody making a trade in Chicago and somebody in Wall Street in order to get the time tag right. So that the guy who made the trade first gets the deal instead of the speed of light getting in the way. Well, I mean, that's a real-life thing today which has to do with, if you don't have the same time, there are real problems. That happens to all kinds of things. So one of the issues that I see coming is, how do we actually use the cloud such that it is a positive security protection system, a positive interoperability system, a positive experience for users who are not going to get overly constrained by the processes that go on top of it from competing empires? All of them perfectly valid, none of them with a serious way to design, in their own minds, how they fit in the rest of the world. That's very different from Microsoft. That's very different from Google. That's very different from commercial cloud providers. We have an experience in the intelligence community. It happened in the last administration. They wanted to save $500 billion. Was that what it was? Some enormous amount of money. Maybe it was $100 billion. And they promised they were going to save it in IT by going to cloud computing and cloud storage and save all the money of all these distributed systems and so forth and so on. And they set it up, and they ultimately put a system engineer in charge, who was the deputy director of National Intelligence, a very wise lady who used to work for me, really knew about system engineering. No question about it. They assigned the job of the desktop environment to NGA, Geospatial...

LINDBERG: Intelligence Agency.

STENBIT: ...Yeah, Intelligence Agency. They assigned the job of the computing to NSA, and so forth. Well, when you build a computer and you're going to have things connect to it, you need to know what that connection is. And NGA published, “This is how we're going to interface with the rest of the world.” But then they ran the procurement, and they picked somebody who didn't meet those standards. So, I mean, that's probably an overstated story, but it's close enough for government work. Things like that are going to happen. And so I'm more curious about how they're going to manage the outcomes, because they're going to have to make trade-offs between user satisfaction, real-life imperatives and whoever the bureaucrat is of the day in whichever meeting. Because there's going to be meetings with five and 10 people and them all having different opinions. How does that actually get done in the real world after there exists a good cloud-based storage, cloud-based processing system? And we can talk about that later. But I'm not optimistic.

F. SCHNEIDER: I think it will be important for DoD to manage expectations and reflect back a decade ago about how computing worked. If you wanted to create some new functionality, you had somebody write a program that you ran on some computing platform. Maybe it was your desktop. Maybe it was some servers that your organization ran. And periodically, we would observe that we had a great diversity of these services, and we would do better to centralize them. So for example, at one point, large fractions of DoD were told to use a particular email service rather than use the one they were using. Or we decided to use a single centralized authentication service. It was called CAC cards, I think. So there were these tensions where there were advantages to centralization and advantages to decentralization of control. Decentralization let independent people come up with neat ideas and run with them.

Moving to the cloud is not going to change any of that. That's a completely orthogonal set of questions. Moving to the cloud will just mean instead of buying a desktop computer or using the servers down the hall, you're going to use the servers that the cloud provider makes available to you. So we should decouple the use of a cloud service as the source of cycles or storage locations from the tyranny, or lack of tyranny, for doing various kinds of centralized management. DoD may figure out a way to do centralized coordination of various functions and they had that problem 10 years ago. They will have that problem for the near and foreseeable future because of the decentralized nature of how DoD is organized with services and a central thing. So we should have the right expectations about moving to the cloud. And if we have expectations that it will mean high centralization of services and so on, that needn't be the case. That's a separate set of decisions.

W. SCHNEIDER: This discussion about security and how it's maintained raises one of the dimensions of security that has not previously been the case here. A number of the players in DoD leadership have begun to emphasize the fact that the homeland is no longer a secure place. You not only have opportunities for cyber operations against U.S. infrastructure, but I'm reminded of the physical vulnerability of the infrastructure for cyber, not only the communications links but, in the case of the cloud the storage sites themselves, where the hardware exists and the processing takes place. This week, the Russians and Chinese have had a large-scale exercise in central Siberia called Vostok 2018. In one region of central Russia, in the Tula-Volga area, they had a mock attack on the power grid. At the same time, they were conducting these large-scale military operations at a training range in central Siberia. So it illustrates the fact that in addition to the kind of

cybersecurity that we worry about day-to-day, we have issues relating to the physical security which are inevitably going to have to be rolled into the way in which we manage this, because of the fact that the adversary will have opportunities to engage the entire infrastructure, not just attacking it at the most vulnerable spot, as has been recently our experience.

LINDBERG: We're pretty far along in a process that is going to lead to an award. What are the key public policy issues that we should be thinking about now as we are ready to make that jump?

STENBIT: Well, I'm with Fred. You need to separate the mechanics from the operation. I tend to think of the problem as there are three elements. There's processing, there's storage, and then there's, whatever you want to call it, the operational integration of the two. So it is how the problem is solved. So one can think of storage being wherever it is, processing being wherever it is, but what you want to do is search, you go to Google, and you take a process that you know how to use. And it goes to the storage, and it goes to the processing. It happens to be their own, but they've already gone out and looked at the Web. So it's that third part that's very, very difficult – very difficult – to manage across a large organization, but if it's not done properly, the security of the whole thing is put at risk. The performance of the whole thing is put at risk. And most definitely bad, it's a historical precedent almost always instead of a forward-looking precedent. And so it will forever...

LINDBERG: So let me stop you there. Tell me what you mean by that, a historical precedent versus a forward-looking precedent.

STENBIT: So I was used to using the telephone, and I knew what a telephone was. And when I wanted to do real-time command and control, I would open up a telephone line to my buddy at the other command. And I would never hang up, so I knew I didn't have a dial problem, and he would be there. He'd have to have somebody there 24 hours a day. I'd have to have somebody there 24 hours a day. That means when trouble occurs, you can't figure it out because you're talking only to the people you know.

I'll give you an example. Lloyd Bucher is on the *USS Pueblo* off of North Korea in 1968, and these North Koreans are coming at him with guns. He has a telephone. Turns out it's not connected all the time, but he has a telephone. He's got a telephone number. It's a plastic-lined sheet of paper. It's got 14 numbers. They're all spooks. Nobody on that list owns a gun. So he called everybody he can, "They're coming after me. They're coming after me." Four days later – four days later – Washington figured out Marine F-4s on Okinawa could get there and bomb this thing and save the thing. But it only took the North Koreans a day to get it back into port. And so he spent nine months there with his crew and so forth and so on. That's the issue of you have a way of doing things. It's historical. It works, but it doesn't work in the next case. It's different.

The opposite is when we went into Afghanistan, which happened to be when I was there last time. We had set up a system that people who had guns listened to a broadcast network, and people who saw targets talked to a broadcast network. And you didn't have to know who was your buddy or who was going to shoot the guy on the left, who was going to shoot the guy on the right. And the very first thing that happened in Afghanistan – there were some special forces that were out on – they weren't out on camels, they were on horses with the Northern Alliance people. And they were having trouble with these guys up in the hills, so they radioed to their guy, which basically relays it to the system. The airplanes that could get there listened. And about, you know, 30 seconds later, the top of the hill blew away. The guy who called it had no idea, "I need to call division, and they need to call whoever," and all the rest of that stuff. It came. That's a very different world. But that was an *ad hoc* world in those days that people are now used to. Power in DoD these days, and to kill people, which is what they actually do, is horizontal. And if the cloud invokes processes or whatever that inhibit that, it's going to slow things down. I'm sorry if that's too long an answer.

LINDBERG: No, that's fine.

STENBIT: But I meant you tend to build what you're used to, and not to build – it's a fundamental flaw of, let me call it, socialism versus capitalism. Nobody's taking risk about the future. It's all looking backwards.

F. SCHNEIDER: So we say things because our heart is in the right place. And sometimes we then move into a situation, and you realize you made a mistake. And you revisit it, or sometimes you have trouble resisting the temptation. And even though you said you would avoid the temptation, you're seduced. If you look at the RFP, it's pretty careful about requiring the performer to provide the capabilities so that we, DoD, does not get caught with vendor lock-in. We have the flexibility to move to another commercial cloud, and we have the flexibility to interoperate with other clouds at the same time. For example, maybe somebody provides a service that the winner doesn't provide, and we'd like to be able to import it. It's going to be very important that we think carefully when we revisit things based on our experience, and we don't make decisions that will inadvertently make it difficult for us to have flexibility moving forward. And the kind of flexibility I think we should think about is not canceling our contract with the winner and going someplace else, but evolving to a community of clouds that are cooperating. The argument that we should start with one because it'd be a good way to get experience and we'll understand the picture better is a good argument. But it has to be an argument that's a first step to us thinking in terms

of being able to take advantage of the whole industry's innovations, and being able to bring to bear the best solutions when we can. It's very seductive to do things in a way that you can't exit a cloud. You might start by deciding, "Well, let's not spend the extra money to build our applications in a way that they are portable, because it's just an extra cost." And you might start by saying, "Let's not run the drills where we move to another cloud for the weekend just to convince ourselves we can do it." And that's a slippery slope. And in some years, it puts us in a lock-in situation. Moreover, the winner has every incentive to promote those kinds of decisions, for obvious reasons. And so this is one of these cases where we are going into this with good knowledge that lock-in would be a risk for many reasons. And we have to be strong about it, and not do the cost-cutting in ways that would compromise that.

LINDBERG: You go.

W. SCHNEIDER: In this study, although most of the public discussion has focused on the process by which the cloud services are procured, we've tried to address three dimensions of it, one of which is the way in which it's procured to deal with the issues that Fred has pointed to. But the other is the security of the cloud. I mentioned the physical security of the cloud, which is not so often discussed but is certainly a dimension of the security problem. But the third dimension is to protect the ability of the government to be able to sustain a process of innovation, so that we can build on the richness of the industry. Because while DoD is moving to the cloud, most of the larger companies have moved to the cloud. And indeed, many of them are – indeed, I think a majority of the larger enterprises – are in multi-cloud environments where they will procure specialized cloud services for specific applications. And as Fred indicated, a multi-cloud environment and being able to manage it that way. And I think that's probably where DoD is headed. Some of DoD leadership has spoken of trying to promote an environment that they describe as fiercely competitive, that will facilitate the ability of the cloud service providers to present to DoD the full range of services they can offer. The temptation that Fred has mentioned about cutting costs is ever-present. The problems that have been generated by the office of the assistant secretary for a systems analysis, or as it's now called, cost analysis and program evaluation (CAPE) is an enduring problem for DoD. And this is going to require some farsightedness on the part of both DoD leadership and the Congress to recognize the enduring importance of creating an environment where storage and processing of data and an environment where these are going to be the dominant features of the conduct of not only military operations, but the operations of the Department of Defense as a whole and, indeed, over time, the entire government is likely to be using these kinds of services. So DoD is something of a pathfinder for this, has a particular responsibility for being able to produce an effective segue to DoD acquisition of cloud services but, over time, the government as a whole.

LINDBERG: John?

STENBIT: Yeah, I want to double emphasize what Fred said. There is an experiment that's run by the government already, and it's operational. That's by the intel community. And they happened to choose to develop two clouds simultaneously, one which was commercial and one which was government-developed. I told you one of the horror stories of the government-developed one, but they both actually now exist. They have interoperability problems. But if I were involved in this procurement, I would not give the contract until the guy showed that he could interoperate with both of those clouds, because that's one they're going to have to interoperate with. And it's not a theoretical problem. The problem will be for DoD to define the test that they will accept as this because you can't just sort of wing it. And that requires, actually, that they tell the contractor the test they're going to have to pass before they start their work so that they understand what has to happen.

I'll give you a counter example. It's called medical electronic records, where the government chose to impose a constraint on the operations, not on the physical computers. Epic, which is a company that's now very rich, built their system to meet the requirements, but made sure that nobody else could ever get them. And if you've ever changed doctors, and you've tried to get your records changed, you discover it's not like pushing a button and getting it sent. So this whole issue of, "What do you do after you have it?" is more than just, "how do I make the programs work and how do I interface with the users?" But it has really significant issues. And you brought up two interfaces. I would pick like that one, pick the bombing data for all of the big strategic areas in the world, which is held in various sundry places, and make that also be a requirement that this cloud can actually go to all of those and have it go to all the guys that have guns that could get to it. I mean, I would have some rather significant interoperability questions that lead to whether, in fact, you could meet Fred's criteria that we can move back and forth if we have to.

F. SCHNEIDER: So Bill brought up twice, actually, the issue of security and physical security for the cloud. And it's probably worth spending a minute or two to understand how that works.

The naive model is that whoever wins the bid is going to have a machine room. They'll hire people. We need to trust these people. They get to wander in the machine room. Whatever computation is going on in the computers is available to whoever wanders down the hall. And they might stop and go look in the memory or detach a disk and take it home.

So that's not how modern clouds are built. And that's not a fear. What you should think about is a building where these racks of machines are in locked cages. There are video cameras pointing to all these locked cages. And the locks don't open while the machines are running. So, if you were a malfeasant employee, and you wanted to get to a machine, you would have to break in. And, of course, the video camera is recording this. While the machine is on, the data might be available. But data that is kept outside of the processor board would be encrypted, right? So when it's stored in outboard memory, when it's stored in disk, it's encrypted. And the only time you get to the machine is when it's turned off. And when it's turned off, all the data that you can get to is encrypted. All the data on the electronics of the processor will have diffused out. And so you can think of *Mission: Impossible* stories where somebody breaks into the cage and has spoofed the cameras and so on. But it's not a matter of trusting the cloud employees. And in that sense, our current machine rooms have insiders that do have access to lots of information and have employees that do have access to lots of information. And there are a lot of sad stories over the last few years of that happening. That's not something that would occur with a cloud provider. Their employees actually need not have access to any information in unencrypted form. And there are good ways to support that. And that's pretty much standard practice now in clouds.

LINDBERG: Well, that sounds terrific. But that doesn't mean the risks have been eliminated.

F. SCHNEIDER: Right.

LINDBERG: Or does it?

F. SCHNEIDER: Well, the risks haven't been eliminated. One risk that is ever-present is availability, right? The location may become available. The second thing is that no system is secure. Some systems are more secure than other systems. And we in security live with that reality. And you have to decide secure against what and what kinds of investments and so on. So what I described was more secure than anything we're running today. And that seems like that's an improvement.

W. SCHNEIDER: Still, the physical security is an issue because, while the adversary can benefit from access to the data, they can deny the U.S. the benefit of the data if they physically disrupt the facilities. I believe this. At least the initial procurement is focusing on three alternative sites. These would be in commercial locations. So although in principle, they could be on military reservations or other ways of improving the physical security, nevertheless, there will be a finite number of these. And as inviting as a target as they are to collect data, the physical security will need to be attended to as well, as we do in other national security sites that are important, few in number and expose the nation to considerable damage if the sites are disrupted or destroyed.

F. SCHNEIDER: So any time you detach the computing capability from the user, there is going to be a risk that the tether can be severed. And to the extent that we currently outsource serving, whether it's to a cloud or elsewhere, we've run this risk. And I think this points to an important distinction between tactical uses of a cloud and enterprise uses. When we deploy someplace, there's definitely not going to be a cloud there for all kinds of reasons. And to the extent we become dependent on using data or processing capabilities that are in this new cloud service for actually fighting, for the warfighter, there is going to be the possibility that those communications lines get severed and availability will be an issue. And we need to design those systems with some capability for graceful degradation, for some Plan B operation. And we also need to make sure we exercise it so that we're experienced in living in that world.

W. SCHNEIDER: In the solicitation, there are provisions for providing cloud services at the tactical edge, which would incorporate the idea of putting some fraction of the capability into a transportable MILVAN or some similar device that could be maneuvered in the theater. But we also know that the communications links are vulnerable. The Russians are reported in the news media to have developed mission equipment for submarines that are designed to cut submarine cables, for example, that are an important part of the ability to move data overseas. So, as Fred suggested, it's a relative security issue. I believe the security of the cloud will be substantially improved over where we are today. But the cloud also introduces other kinds of security concerns that have to be incorporated in how we operate.

STENBIT: I think, since you've hit a nerve of mine, when we were building this system for DoD back in the beginning of the Afghanistan, terrorist war – whatever you want to call it – we clearly recognized that the tactical edge needed help. We had a program on the drawing boards called TSET. I don't even know what the T stood for. But in any case...

LINDBERG: Tactical.

STENBIT: Tactical. It was exactly to provide anti-jam communications to people in the field.

LINDBERG: To provide what? I'm sorry. To provide what communication?

STENBIT: Anti-jam. Secure, can't be jammed by the Russians, can't be jammed by the Chinese via satellite. Satellites could get blown up. That's part of this whole issue. But it was a mechanism to, along with the defense of the satellite training problem, to be able to solve this problem was that we were going to use lasers. It was really a high-tech thing, cost a lot of money. It was canceled, which happens quite often when there are things like this. But it turns out the commercial world is providing it these days. So the reality is that commercial satellites that are up there flying, and you can go rent it and put it on your roof or whatever you want, put it on the back of your Jeep – are providing systems that have better AJ – anti-jam – capacity than DoD's satellites, and they're doing it because they want to make money, so they keep the beam separate. It's a whole different world out there. I actually, well, it's a conflict of interest: I'm on the board of a company that does that, so I'm a little bit zealous on this. But I personally do not believe long-range connectivity to wherever you want to put the cloud. Cloud connections is going to be a problem five years from now. And I don't think the cloud will be effective by five years.

LINDBERG: Where do we want to be two years from now? What kind of a conversation do we want to be having? How will we know how well we're doing once this contract is out?

W. SCHNEIDER: It seemed to me that we want to be able to show that both secure storage and operations can be conducted in the cloud and that we have a template for how the cloud procurement can assure DoD access to the innovation that's available in the private sector, and that DoD has an acquisition process that facilitates DoD's acquisition to a vibrant commercial market. And I think the path that DoD is taking, where they are emphasizing the need for competitive procurement in the long term, I think, is going in the right direction.

LINDBERG: Fred, where do we want to be two years from now? What are the questions we want to be asking? What answers do we need to see?

F. SCHNEIDER: I'd be curious to see, first, who's moved, and what's gone wrong, and to be prepared to learn from that.

STENBIT: I go to another of my nerve endings that are exposed. DoD does a good job of doing large, let me call it, information training exercises. They're usually called command post exercises, where they run scenarios against rather sophisticated kinds of issues. They're world-wide kind of things. And one of the issues that I always wanted to test was the anti-jam capacity of the communications. And so it's easy: you go and you pull the plug. And you simulate that that has been jammed. Well, it turns out these same very large-scale operations are part of the training issue of the people, and so they have to get through these training exercises in order to get the check mark that says they have passed. Therefore, you are not allowed to just pull the plug, because they won't get their pass because they didn't actually succeed in the exercise, because the communications were disrupted. And so you don't test the actual utility in the disrupted state in order to protect the training bureaucracy's check marks. What I would like to see in two years: serious people attacking the edges of this system in a real scenario and having them not go through the training exercise but go through the red team exercise of, "Oh, look at that. I broke you, and it only took me 32 seconds."

W. SCHNEIDER: Until about five years ago, when you had a military exercise and introduced cyber operations, it was the end of the game, because it shut the...

STENBIT: Well, that's the same thing. Jamming and denial of service are the same thing.

W. SCHNEIDER: Yeah, right. But then, DoD Joint Staff decreed that they had to play the game through and they had to work through a cyberattack. And I think now it's moved to the cloud. The point that John makes is especially pertinent because of the dependence DoD will have on cloud-based architecture.

LINDBERG: I think we've got about 20 minutes, so we can take some questions. And if you'll do us a favor, waiting for the microphone, and maybe you'll introduce yourself. And we'll proceed. Thanks.

UNIDENTIFIED PERSON: First, thanks for the interesting discussion and important discussion. You explained the fact that the RFP asks and requires the winner of JEDI to ensure portability and flexibility, but you also described some of those ongoing risks and temptations and even incentives for the winner to lock-in those applications and data on an ongoing basis through cutting corners or otherwise. What, if any, are the policy tools that we can put in place now to ensure that we don't end up, down the road, having future lock-in issues, even though right now the solution requires portability and flexibility?

LINDBERG: Great question. Thanks.

F. SCHNEIDER: So with all due respect, and no offense intended, Red Hat is pretty low in the software stack, and many applications are way above that. And there's the risk that lock-in is going to happen not because of the lower levels but because of the particular enterprise application that's chosen. If we required that any program that manages a database has the capability to export that database into a portable form, and if we, even in addition, provided that there was some

kind of input filter so that it could be ported to some computing application, that would be a way to liberate us from vendor-lock.

STENBIT: I'm going to go back to a history of Red Hat. So I defer to you that you fixed all of this, OK? But back in the good old days, you were an open-source operating system attempting to create an environment which was very conducive to what you were talking about. And we kept saying, "How in the world are we going to secure this, because they change it every other day?" And we had a big argument about, "Will you ever manage configurations long enough so that we can actually trust it?" And there was a whole going-around. Even worse, I personally had money spent to teach you guys how to secure your operating system using the data that we know from NSA and some other places. Now you can claim you didn't need it, but certainly, the performance of the system after we spent the money was better than it was before. So I believe the issue that I would like to generate from that – not picking on you, because you've been very successful at doing a lot of things that are noble and good – is it's the key that the knowledge that the government has about their special cases gets shared appropriately with companies that are making their money in one way preferentially over another, because that's how what you've been doing is a very important issue, and it has to do exactly with the interfaces we've been talking about, between the reality of a hardware suite and the actual getting the operations going. And I don't mean any bad reflection on Red Hat, but there are always trade-offs that are involved in all of this.

LINDBERG: Please. Yeah. Go ahead. Microphone? Please wait for the microphone. Yeah.

UNIDENTIFIED PERSON: I'd just like to respond. Our work with NSA has made us even more secure than any of our competing...

STENBIT: That was our intention.

UNIDENTIFIED PERSON: Yes, so thank you for that.

LINDBERG: All right. So if you want to ask a question here, it's at one's peril, but we'll have another question. Yes, please.

UNIDENTIFIED PERSON: Hi, I'm […] with CIO Dive, so I'm coming from a more tech perspective on this. While the vendor contracting system in federal acquisition is fraught with politics, I think we've seen it come into play a little bit more here. And I think, with the JEDI contract in particular, something that has been neglected is the actual technology that some of these providers can offer. So, I mean, we haven't even having finished the RFP process, and there's already been protests against the bid, in particular from Oracle. And the whole narrative tends to be, "We want a play in this game too; the giants shouldn't have it all." But then I think we're coming to a technology capabilities question. And so can you speak a little bit about the actual vendors at play? And then also, who is capable of these offerings as opposed to what's being politicized with a contract RFP process?

LINDBERG: Would you want to talk about that a little? Just as an answer, you'll find this in all of the material that we have that we at Hudson have produced on the subject. In light of this question, in particular, I'll mention that we have undertaken this project with the support of Microsoft and Oracle.

W. SCHNEIDER: From the media coverage, which is the only source I have on it, there's several of the major players, including Amazon, Microsoft, Oracle and perhaps IBM as well that have the scale and are close enough on the security required by DoD to be able to respond to at least the initial offering. But DoD has not yet published the roadmap of how they're going to proceed in the way in which they build up a network of cloud service providers.

LINDBERG: Let me just interrupt you for a second. This is the second time you mentioned a roadmap. What is the significance of a roadmap in relation to a contract like this?

W. SCHNEIDER: It's become a practice of DoD to give vendors, as well as the Congress, a long-term perspective on how a particular suite of programs or capabilities are going to be managed. For example, they just published a roadmap for the way in which DoD is going to procure unmanned systems between 2018 and 2042. Some systems, of course, are more amenable to long-term forecasts of that sort. And so DoD has a roadmap, but they haven't yet published it. So I have no insight as to exactly what its content is, but because they talk about maintaining a fierce competition for these services, I deduce from that they have some plan to expand the scope of cloud service providers from what might initially be a relatively small set of large firms that are capable of responding to the RFP to a process yet to be described, about how the larger cloud service industry will be integrated into DoD concept for procurement.

STENBIT: I think you can go to any strategic planning course, and one of the President Bush's, I think it was the first one, said that vision thing. But you need to know where you're going, and then you can have some view of how to make the

trade-offs. I don't think DoD has adequately described where they're going. And I think it's those kind of issues that we've been talking about. Some elements...

LINDBERG: Are they holding out on us, or is it because they don't know?

STENBIT: Well, in general, DoD doesn't do things like that. They talk about procurements that are now, and they talk about research which is the future. I mean, look. I've worked in DoD twice. They're like any place else. They've good stuff and bad stuff. But in your particular case, I think you do need a strategic plan that says, "Are we going towards just the mechanical part of the processing and the storage, and we're going to count on some other system to be able to manage all of the operations? Or are we going to embed it because we want to do big data analysis as part of this because we have an enabler?" That's a very different definition of what the job is, because there are more people who contribute to big data analysis than the people that do cloud centers. So I think this whole issue is what I always used to say. On any procurement, I want to know what's the test that I'm going to do at the end that if they pass, I'll pay them, and if it doesn't pass, I won't. It's a good question to ask.

F. SCHNEIDER: You know, good advice in this town is about follow the money. I'm prepared to bet that the provider of the cloud's platform is not where all the money is going to be. The money is going to be in the services that run on top of it: Salesforce, or what have you. And we haven't heard anything about that. But that's the way to make a fortune. And that's the way that smaller players are going to be able participate. So this is just creating the environment in which that kind of ecosystem can flourish.

UNIDENTIFIED PERSON: Good morning. My name is […]. I think it was Fred, who mentioned access to innovation from and through the private sector. Is there a true connection between these commercial cloud providers and access to innovation? If there is, great, I'd like to hear more. If there perhaps is another way, if you could talk about that. I really come from talking to people like General Dash Jamieson and some other folks that are in that community that are just hungry for innovation. They believe it does not come from the industrial complex anymore. It comes from the private sector. Just your thoughts on that.

F. SCHNEIDER: So it's interesting to contrast, say, the Microsoft cloud and the Amazon cloud. Amazon makes money when other players in the private sector build services that they deploy on the Amazon cloud. Not because the author of this service necessarily pays Amazon; it may be that the customer pays them. So this is a way that Amazon wants to encourage this sort of thing. And that means Amazon wants to encourage lots of connectivity to their cloud. It means Amazon wants to encourage us all to have smartphones because of that. All right, OK.

So the Microsoft cloud is originally designed to promote Microsoft services, so it runs Windows and so on. I would be surprised if they are betting the company on everybody adopting Windows Office and so on for their long term. I think if you look at what Microsoft's been investing in, it's been in machine-learning models and the capability to be very efficient about helping people to build new models to manage data. Right? They do that. They will sell you the data, they will sell you the model, and you'll end up buying their services.

So both of those, they're two different very, very different clouds. And yet in both cases, they are depending on the private sector to use their infrastructure to sell services to the customer base, which in this case would be DoD. So, if anything, this is a very nice level kind of playing field, where smaller players can participate because everyone has access to these clouds. And therefore, you can do the design and debug and so on.

STENBIT: In the old days when DoD controlled all of the electronic and software kind of innovation in the '60s and '70s, contractors would do work for DoD and then marginally price what they learned into products that were actually useful on the outside. Now, a lot of those failed, but that's what happened. Today it's the other way around. And I think Fred was just talking about it. DoD is marginally pricing all the technology that's gone into these big cloud storage and computing facilities, done for different reasons with different strategies, different end games. But they're trying to marginally price that and make it cheap on their side. That's good. That's the good part of all of this. Nobody picks up government bureaucracy as their model of getting future things done.

UNIDENTIFIED PERSON: Yes, hello. […], I'm a reporter at Politico. You know, I think everyone's well aware that DoD has received a certain amount of criticism for taking a single-source approach, at least to this initial award for JEDI. One of the department's responses, at least that I've caught, has been, firstly, the JEDI contract is only going to cover less than 20 percent of the department's web-hosting requirements. They've also made a point that I think, Professor Schneider, you have made, which is that there's going to be lots of opportunities for service contracts as a follow-on. So I'm curious what all of your kind of take on this debate is, as a first question. And secondly, for somebody like myself, trying to kind of get their arms around as much as possible the totality of the different DoD clouds out there, is there a resource that sort of weighs this out that you would recommend?

W. SCHNEIDER: It's a hard question to answer. I think when DoD publishes its roadmap of how it intends to proceed, it would be easier to divide it because now it would be a few alternative hypotheses about how DoD might choose to develop the cloud. And certainly, the rhetoric that DoD has used around its effort to solicit cloud services has emphasized, in particular, the idea of assuring a competitive environment. And so I think we'll be able to give a better answer to that perhaps after the solicitation is completed, and DoD has a more fulsome opportunity to explain where they're headed. This is really a bet-the-department kind of initiative, because that's how the department is going to be operating for the foreseeable future. So I'm confident that they will explain themselves in more detail in due course.

F. SCHNEIDER: You did say DoD has many clouds already. So a better way to look at this is DoD is getting a contract to get another cloud, not *the* cloud. And as long as they view it that way, and it's the first step, then I think we'll be in very good shape.

LINDBERG: OK. Do you have a point to resource for...

STENBIT: Me?

LINDBERG: No, no. The second part of the question was...

STENBIT: Yes. No, I understand. The answer is no.

LINDBERG: The answer is no. Well, nice try. Sorry. You got anything...

STENBIT: I think this is the place to go look. They run the consolidated data centers, which is as close as they get to clouds, I believe.

LINDBERG: Yeah. All right. Well, we're just about out of time. Let's just go back, and I'll ask each of you what you think we've missed in the discussions so far and ask you for maybe a minute on that at most. I mean, I think we've brought a lot of issues to the surface here. There's obviously the sense that we've got a moving target and that it's very much a work in progress. As I come back to this term, pathfinder. That's because there isn't exactly an obvious path for an undertaking of this magnitude.

F. SCHNEIDER: So one thing that was missed is long-term consequence of migrating enterprises to the cloud. As we become dependent on enterprise applications, that means disruption can disrupt our warfighting efforts. And it becomes possible for our adversary to plant stuff in these enterprises over a long period of time and then invoke them as a way of preparing the battlefield before there is an attack. So it's not very cloud-specific, but it is consistent with our march to increased automation that we are going to have risks not only in what you would think of as the high-consequence applications targeting and so on, but really low-consequences ones like deploying materiel and scheduling transports and things that aren't generally thought of as high-secure things, but nevertheless could be highly disruptive. So we will need to migrate these business functions in a way that they are more secure then we worry about today. Thanks. Bill.

W. SCHNEIDER: We just scratched the surface of the implications of the large-date integration of data and processing to cloud-based architecture. DoD evolution to employing the technologies in autonomy, for example, have just begun, and they're not even really tactically fielded as yet, but over time, they will be extensive. So the understanding of how the organism will operate, where most of the data is generated and processed outside of the platforms that are engaged in tactical operations, or the support of military operations, or the support of business operations of the department is a new world for DoD. But it's one that is likely to be replicated elsewhere in society with governmental institutions, as well as private sector institutions increasingly operating in this manner. So it's very important that we begin to get our hands around the full scope of this issue.

LINDBERG: John.

STENBIT: There's a general rule about DoD procurements. They are given birth by a semi-infinite number of meetings with all kinds of people – not the same people all the time – with conflicting ideas. It ultimately comes out as a consensus of negotiation of adjectives that go in the RFP. Not numbers, not facts, not requirements, but adjectives. A lot of DoD programs that are revolutionary really blow up in cost and schedule rather quickly and catastrophically after such RFPs. The ones that have been really successful have been those – and I'm not recommending this at the present moment – when Congress or somebody has cut the funding at the front end of the program right when it was announced, and that the contractor and the government had to skinny down to a level of effort of, let me call it, system engineering and program definition and, "what am I going to test at the end?" and a whole bunch of discussions that have not been done at the adjective level, but at the real level. And then the process is that the government has to buy on to that as the new definition. And those programs are much more successful. So one that's this complex, I don't recommend that we cut the funding, because that has all

kinds of other kinds of implications. But I do recommend that the government spend as much time worrying about how they're going to figure out whether this is what they wanted, and use all of those arguments about what does the testing look like, and then do a cost analysis of whether you can test it or not. And this program will be a lot better.

LINDBERG: All right. John Stenbit, Bill Schneider, Fred Schneider, thank you very much. Thank you for joining us. Those of you who've have been watching online, glad to have you, as well.

W. SCHNEIDER: Thank you.

(APPLAUSE)