Hudson Institute

Requirements for a Successful Military Cloud: Best Practices, Innovation and Security

- William Schneider Jr., *Senior Fellow, Hudson Institute*
- Tod Lindberg, *Senior Fellow, Hudson Institute*
- Seth Cropsey, *Senior Fellow and Director, Center for American Seapower, Hudson Institute*

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
July 30th, 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/1582-requirements-for-a-successful-military-cloud-best-practices-innovation-and-security72018

TOD LINDBERG: Hello and welcome to Hudson Institute. I'm Tod Lindberg. I'm a senior fellow here. I work on national security policy and related matters. Welcome to our discussion today, Requirements for a Successful Military Cloud: Best Practices, Innovation and Security. We have two very distinguished panelists joining us today. Bill Schneider is a senior fellow here at the Hudson Institute and is president of International Planning Services Inc. He was also chairman of the Defense Science Board. And Seth Cropsey – he's a senior fellow here – is director of our Center for American Seapower. Seth's background also includes a stint as deputy undersecretary of the Navy in the Reagan and Bush administrations, and then in the OSD, the Office of Secretary of Defense, in those administrations as well. I'm happy to welcome you all here.

Obviously, as many of you know, this is a subject that had a major news events associated with it last week. And so I thought what we would do is just begin by having Bill Schneider give us a little précis of that. And then we'll get on into the broader questions of acquisition at DoD, and, in particular, the issues that are surrounding the military cloud aspect and the current state of that debate. So, Bill, what's going on out there?

WILLIAM SCHNEIDER: Well, it indeed has been an exciting time for innovations in the Department of Defense. About two months ago, the department, at the urging of Deputy Secretary Shanahan, initiated a draft request for proposal for the DoD procurement of cloud-based information technology services. After receiving industry comments and congressional comments, it stood down for about two months as it reviewed the entire subject. And then late last week, it published a final version of the request for proposal. The offers, in what is described as a free and open competition, have until mid-September to submit proposals for a firm-fixed price to deliver cloud services. It can be for a period of a minimum of two years, with extensions and renewals up to a period of 10 years, for an estimated cost of approximately $10 billion for the cloud services that would be rendered to the Department of Defense over that 10-year period. So it's quite a change, in that DoD has been discussing this for a decade, but has been relatively slow to move. So it has been greeted with a great deal of interest.

LINDBERG: Great. Thank you, Bill. And now, Seth, let me turn to you. You've had an insider view on questions related to the DoD procurement process, and, in addition, you've supplemented it with years subsequent to your service in government and researching in this area. I fear that if legislation is like making sausage, DoD procurement is like – I'm not sure exactly what that would be like...

SETH CROPSEY: Sausages without the casing.

LINDBERG: Sausages without – yeah, OK. So, how about telling us a little about this process?

CROPSEY: Thanks, Tod. I think a good way to start thinking about Defense Department procurement is just to get a glimpse of the size and the scope of defense agencies that come under the secretary of defense's control, which have been established over three, four, even five decades. I'm not going to read the whole list to you. I'm just going to read a little bit of it. But this information is very important because procurement is, well, let's say it's essential to the defense of the country. And it is one of several important issues that are governed by and controlled by different agencies. So we have the Defense Advanced Research Projects Agency which only has 220 employees; we have the Defense Commissary Agency, which employs 18,000 people; the Defense Contract Management Agency, which has almost 12,000 civilian and military employees; the Defense Finance and Accounting Service – I'm sorry to say, I can't tell you how many thousand work there; the Defense Health Agency is also large; there's the Defense Information Systems Agency, with 8,000 civilian and military employees; the Defense Contract Audit Agency, which employs 5,000 people; the Defense Intelligence Agency, which employs almost 17,000 people; the Defense Logistics Agency, which, for example, handles all non-military items, like pencils and toilet paper and things that don't have military requirements, which employs 27,000 people.

So I'm going to stop there, because I wanted to give you just kind of a sense, but the list is a lot longer. It's two pages. Leaping ahead somewhat, it's likely that, when cloud computing arrives, each of these would have to be integrated into any cloud system, and that is not free. So with this list fully, the total of people here is somewhat smaller than the Marine Corps. That's a lot of people: 150,000 here, 186,000 or so in the Marine Corps. These have multiplied as DoD bureaucracy has expanded. There was a time, way back in the mists of history, when the military services were primarily responsible for building designing, and constructing platforms and weapon systems. In the early 1960s, Secretary McNamara migrated partial responsibility for design construction procurement into the Office of the Secretary of Defense. The Goldwater-Nichols Act of 1986, not quite so old as McNamara's administration at Defense, gave geographic commanders, which were then called the Syncs, more say in Pentagon decision-making, so that it added more cooks to making the stew. The Joint Staff has their own requirements element. The military services maintain some control over procurement decisions.

And, as amazing as it may be, things don't always work out the way they were intended. Just a very, very brief example: in the Reagan administration, and with the help of one of the shipyards in the South, Congress decided to tell the Navy to spend $100 million and appropriated money to build a replacement for a Vietnam-era small boat. And the procurement system, even in the 1980s, was complex, and accountability was iffy. What ended up was a 331-ton vessel that was subsequently not used for the

intended purpose. And more money had to be appropriated to produce the replacement for a smaller boat that had been used by Special Warfare and which had become obsolete. So this is an example of the fact that Congress is also one of the players in this procurement, this multilayered, complex and largely unaccountable procurement system.

To give you another example of the complexity – but more the non-accountability of this system – some of you may remember that when Admiral Greenert, the chief of naval operations several years ago, was testifying before Congress, Senator McCain asked him to explain the reason for the $2 billion cost overruns of the so-called Pathfinder Ford-class aircraft carrier. And the admiral, who's an honest man, said it's difficult to say so. And he was telling the truth. He couldn't really provide the answer. Decisions about new technologies shift around. They shifted around then, they still shift around between the Navy, between congressional impositions, between the Office of the Secretary of Defense and the Joint Staff. The Ford, for example, the aircraft carrier, does have an electromagnetic catapult and recovery system. It's a new technology. But accountability in its design and construction is not there. So identifying who is actually responsible in the procurement of weapons and platforms is spread out. It's like trying to look at the Soviet's Gosplan and figuring out who decided how many tractors should have been built in 1975. Attempts to control procurement costs in the past have included requirements – and this is a sensible one – that any change orders larger than a $100,000 would have to be signed – this is in the Navy – by the secretary of the Navy and the CNO.

LINDBERG: The CNO is...

CROPSEY: The Chief of Naval Operations.

LINDBERG: I'll be doing that a lot. It's inevitable in the course of discussions of these things.

CROPSEY: So that's a small attempt at trying to control the costs, which invariably arise as a new ship, for example, is being built. It takes a long time to build the ship, even a relatively small one, and technology advances as that happens. And the people who are making the ship figure out different ways of doing things. And they come back, and they say, "Well, this is going to cost more." And so what was attempted 20 years ago or so, was to require requests for change orders to be signed at a certain level – above a certain level – by the secretary and by the chief of naval operations, which was some attempt to put accountability into the system. The process for procuring cloud computing is, ironically, an example itself. The Joint Enterprise Defense Infrastructure, called JEDI, is a projected 10-year – you'll hear more about this – $10 billion effort to switch to DoD from its current usage to cloud computing. So responsibility for the program began with a Cloud Executive Steering Group, established by the deputy secretary of defense. And from there, responsibilities shifted over to the Defense Digital Service, with the unfortunate acronym of DDS, so it reminds you of your dentist. And now, it rests with the Defense Department's Chief Information Officer.

Summing up here briefly, cloud computing has the extraordinary potential to simplify the accumulation and retrieval of data in the Defense Department, sensibly implemented, and you'll hear more about that in a moment. It can save money and time. And it can improve efficiency. It will be most effective if accountability can be returned to the procurement process. Thank you.

LINDBERG: Thanks, Seth. Bill, over to you.

SCHNEIDER: OK. Well, thank you. And one of the important bits of recognition that needs to be afforded to the decision to release the request for proposal is the importance of DoD actually making a decision to begin to move DoD operations to be supported by cloud-based information technology architecture. This had taken on a sort of NATO characteristic, as I call it – no action, talk only – for nearly a decade. During my service in the Defense Science Board as its chairman, we had quite a few discussions about this, because, as you may recall, DoD was moving towards a network-centric concept of operations that had been building up since the 1980s, as a way in which DoD would operate. But I really congratulate DoD leadership, and especially Deputy Secretary Shanahan, for actually biting the bullet. We'll have some additional commentary about aspects of this decision, but the decision to move forward is very important.

And it's important among a number of reasons, quite apart from efficiency and cost, which remain to be seen. But the nature of modern military operations will no longer permit the use of modern military systems without cloud-based sources of data, not only for storage and retrieval, but at least, and perhaps more importantly, for processing. A lot of these data come from many different sources – from space-based platforms, from airborne platforms, naval vessels – both surface and submarines, as well as terrestrial systems. These need to be integrated. And the data needs to be processed, and insights extracted from them and distributed to the combatants to be used. But similarly, data needs to be collected, stored and processed to run the logistics system and many other operations of the Department of Defense. And the idea of moving the data to a cloud-based architecture is necessary for military operations to take place. The F-22 and the F-35 aircraft are two of the poster children for the importance of moving to a cloud-based architecture, but they are by no means the only ones.

As we get into the discussion, there are, I think, three major points that might be addressed, and I'm sure more will come out in discussion. But the first deals were the issue of best practices. If you go through the request for proposal package, one of the

points that comes out is that DoD wants, to the greatest degree possible, to build on the commercial market for cloud-based services. This market has grown remarkably in the past decade. And, as a commercial product, it is quite mature. In fact, more than half of the enterprise-wide users of cloud services have at least five different cloud service providers for different applications. One of the characteristics of DoD solicitation, however, is that they are seeking a single cloud service provider. And this differs somewhat from the commercial model that has been able to take advantage of an industry that's very vibrant, that is capturing new technology, that's developing very rapidly, and that's able to offer it in a service mix that is well beyond merely storing, permitting retrieval and processing of the data. And the market has evolved in that manner.

Another motive for moving to the cloud deals with the issue of security. When Director Clapper, as director of National Intelligence, made an early decision in 2013 to move all of the operations of the 17 agencies of the intelligence community to a cloud-based architecture, it was driven by two concerns.

First was the security problems that had emerged with a decentralized information technology sector that was producing significant losses in data. The failure to patch a computer or a mistake in using a thumb drive to take data off a specific machine was producing problems that could be stopped simply by moving to a cloud-based architecture that eliminated the decentralized property of it. But it was also a question of cost. And Director Clapper believed that the intelligence community could save about 50-percent of its costs in IT services if it moved to a cloud-based architecture. These circumstances were, I would say, generally well-received by the intelligence community in terms of its application, even if the optimism about cost savings didn't emerge as planned. Nevertheless, initially, the movement to the cloud looked successful, but as time went on, the intelligence community found that it needed more than one cloud provider. And, most recently, the intelligence community has lent a contract to Dell and Microsoft to provide another cloud for its application. So I think that with DoD usage of cloud-based services, even though smaller agencies have initiated some cloud-based procurements, a DoD-wide cloud is an immature aspiration and probably will evolve over a period of time.

The second issue relates more generally to some of the contemporary concerns about security. And those issues have the property that the cloud poses still important problems for security for DoD. The first is the issue of the insider threat. The insider threat now is already a formidable problem, as we've seen by spies such as Snowden, who took 1.7 million documents in a very short period of time from the intelligence community, and is now a resident in Russia, after spending several days in the PRC en route to Russia, with his haul of purloined documents, albeit in electronic form.

So the insider threat is an important security issue. But another security issue that will be present on a scale with cloud-based architectures that is not so apparent in a decentralized architecture is the physical security of the installations. The request for proposal calls for a minimum of three such structures. Their location could be on a military base, or at some suitably concealed location. But nevertheless, a relatively small infrastructure like that is vulnerable to physical attack, and a physical attack is quite likely, given the very inviting target that such a high degree of centralization of core operational data is. But also, the fact that these small number of sites, whether it's three or 30, is still a small number of sites compared to the decentralized model. It will still produce an inviting problem for an adversary, and a vexing problem for us.

The third aspect of it deals with supply chain security. The infrastructure – both hardware and software – need to be continually refreshed to respond to both user needs and mission requirements, as well as the evolution of technology. And the problem of preventing supply chain contamination is a very difficult one. And indeed, in some units in the Department of Defense, they recognize that it's not possible to protect the supply chain, or at least that it's not possible to have confidence that the supply chain has not been contaminated. And so other measures need to be taken. With the cloud, where the infrastructure that will be holding and permitting retrieval and processing all of the data of the Department of Defense, the significance of the supply chain contamination reaches a new level of concern, which I think will have to be addressed as the process evolves. And some mitigation of these risks may be possible, if DoD approach evolves from the initial cloud monoculture to a multi-cloud environment, as is used by most of the commercial users, at least at the enterprise level.

And finally is the issue of innovation. The underlying technologies that shape the ability to provide greater functionality with cloud services are changing much more rapidly than DoD processes can permit. So I think the reliance on the commercial sector to provide cloud services is probably a good one from the question of capturing those changes, but the acquisition process needs to also have the capacity to render it attractive for the commercial sector to continue to offer innovative services. In some of the industry comments on the draft request for proposal, it was observed that it's unlikely that the cloud services vendors could make any money until somewhere between the sixth and 10th year of the proposed contract. Well, those kind of rigidities in the contracting process would probably not offer much of an incentive to the cloud service provider to provide additional services and functionality in the absence of some better way of the government procuring such services.

So there's a risk that has to be managed about trying to allow DoD to take advantage of the vibrancy of this market segment, and in providing more functionality to cloud services, because, as is implied by the fact that DoD wide we're going to go to a cloud-based IT model, we don't fight as an Army, Navy or Air Force. We fight jointly, and all of the ability of the military

departments to operate jointly in the fight needs to be enabled. And the cloud-based IT model perhaps presents the most appealing way to enable this. And so, I think, in the longer term, we can be optimistic that DoD's initial steps, even though it's likely to evolve in the way the commercial model has evolved: from initially single-provider as the enterprise became comfortable with the notion of cloud-based applications, and then later to a multi-cloud environment where it attempted to optimize the mix of cloud service providers to meet the requirements of a company, or in the case of the Department of Defense, I think, eventually, to meet the mission requirements of the Department of Defense. So I'll stop there.

LINDBERG: That's great. Thanks, Bill. Seth, there is no commercial market for a Ford-class aircraft carrier, whereas in the case of the cloud, we have a very vibrant commercial market that exists for the provision of these services, at least in a private sector sense – in other words, without sufficient attention being paid to issues related to classified information, etc. But I wanted to ask you, what difference should it make or does it make that this is a thriving commercial enterprise at the moment, as opposed to sitting down and trying to design a new aircraft carrier?

CROPSEY: You mean that, what difference does it make that we're talking about using cloud computing for the military as opposed to commercial purposes?

LINDBERG: Well, no. I meant the internal process. I think when you're sitting down and designing an aircraft carrier, you're not actually working with stuff that's already out there. You've got existing programs, existing procurement, etc., underlying it, but the process itself is different from what you might be doing in terms of acquiring services from the commercial sector.

CROPSEY: The military works with contractors, subcontractors and tertiary contractors on all sorts of things that don't have directly military applications all the time. Computers are one example of that. And, as far as the military procurement system goes, it has a lot of experience, not only with its own – for example, in the Navy, ship builders, Navy shipbuilding – but with companies that have been doing this for, you know, some of them for over a century. So there is a difference. I think Bill's points about security here are vital, because what we're talking about is putting the brain of the U.S. military outside of the military. And that means everything from the design of weapons and, if compromised, the ability to compromise those weapons systems, to, for example, our nuclear planning. And that presents a challenge that is different from the mere building of an aircraft carrier.

SCHNEIDER: The Department of Defense has had a troubled relationship with information technology. If you look at the origins of the seminal inventions that emerged from World War II, it was the military applications of atomic energy and computing. And both of these at the outset were, of course, dominated by the government. And the realities of the almost universal applications of computing compared to the military applications of atomic energy meant that the computing business was going to be driven into the commercial sector. And as we've found since the 1970s, DoD has become a minor user of computing, not a driving user of it, and this is even more so today. So the fact is DoD increasingly has been obliged to adapt commercial technologies to its needs. And to an increasing degree, the technologies that are shaping the commercial applications of IT are moving along much more rapidly than the DoD capacity to absorb them. And one of the benefits of moving to a cloud-based system, especially if it's built in a multi-cloud environment and a competitive acquisition process, is that DoD will be able to capture those advances in technology that produce greater functionality and support for the DoD mission. But the process of getting there is difficult, as Seth was commenting. The DoD processes are made for an industrial age, and they are not made for an age where information is the dominant mode in which the Defense Department operates.

LINDBERG: Bill, this is called a pathfinder contract. What does that mean, and what should it mean?

SCHNEIDER: Well, I think the pathfinder concept does probably not have a definitional rigor in the federal acquisition regulations, but it is clearly providing the image of a little more than an experiment, but certainly way less than an enduring commitment. DoD, as an immature user of cloud services, especially on an enterprise level, needs to advance from the idea of an experimentation with a single purchaser, as was the case with most of the early commercial adopters of cloud services, into one that will have multiple providers providing a wide range of functionality that can be optimized to all of the different mission needs of the Department of Defense. So I think the pathfinder concept at least reflects the fact that DoD does not want to be permanently committed to one approach to cloud services and only to find that by locking themselves into a single approach, they will in fact deny themselves access. For those of you who have had a long term of service in this market, especially with Defense, you may remember back in the late '70s, when DoD adopted the Ada language as what it thought would be a universal language that could be applied to writing code for defense products, and even modern weapons systems like the B-2 Bomber had its code in using the Ada language.

Well, it turned out that was not a good idea, and that had to be sent over the side, as they would say in the Navy, pretty quickly. And DoD's made a lot of these bad bets in its effort to adapt information technology for its own purposes. And so I think the pathfinder concept, if it meets the sort of a common understanding of the term, is probably a good way to proceed, in that they will have an opportunity to assess DoD needs and its adaptation to the use of cloud services, and then move to other acquisition

models, or perhaps other models of how cloud services are going to be used by the Department of Defense, in order to make a later decision on how DoD data will be managed, stored and processed.

LINDBERG: Great. We've got ample amount of time for questions, and I'd like to turn to those now. But as the microphones are coming forward, let me just ask one other question for both of you. The Marine Corps is more or less specified as kind of the proving ground in this Pathfinding period. What significance do you attach to that?

SCHNEIDER: It has a good bit of logic behind it, in that the Marine Corps operates an Air Force-like thing. It also operates ground forces, and it operates at sea. So on a smaller scale, the Marine Corps has all of the problems and issues that the three military departments have, without having to have subunit experiments in each of the services, which I think reduces the enterprise value of the experiment.

CROPSEY: It underlines an importance that people who are doing the decisions here attach to getting the system right. It also, at the same time, draws attention to how important getting it right is, because if the Marine Corps has a problem with logistics, the country has a big problem. That's a large part of what, I mean, what is necessary, so that the Marines can do what they're supposed to do. If they can't get the logistical train right, it's bad.

LINDBERG: Please introduce yourself. And I'll make the usual remarks about brevity. If people go on too long, we'll take active measures.

(LAUGHTER)

AUDIENCE MEMBER: Thank you very much. [...]. Great comments and thoughts, gentlemen. A couple observations. The first pathfinder was supposed to be USTRANSCOM, and they did succeed in getting that awarded sole sourced through a DIUx that attempted to go full-scale in operation very quickly to sole sourced Amazon, which got blocked in courts. Which, you know, one wonders, you know, makes me question, why do we need another pathfinder? The second question is, why so focused on commercial cloud that's public, versus commercial clouds that can be private and more secure? DoD doesn't seem to want to embrace what the commercial market does is something they have control over for their most precious data.

SCHNEIDER: Those are, of course, very pertinent questions, and I think it does reflect the fact that this enterprise or effort to move towards an enterprise-wide experiment with the cloud is what's on the mind of the leadership. What kind of problems are going to emerge? And I think the problems will become evident. DoD security concerns are not necessarily obscure, and even though they may have some unclassified security guidelines, it conceals more than it reveals about exactly how DoD is going to combat it. But I think the security concerns I mentioned are really generic security concerns that affect whether it's a decentralized or centralized kind of system. And DoD is going to have to provide confidence that the move to the cloud will be associated with better security than they've been able to engineer with the existing decentralized cloud system.

LINDBERG: Bill, you made a rather piquant observation a little bit earlier, which was that maybe we can't really make the assumption that there is going to be security. What does that mean, and what are the implications of that?

SCHNEIDER: Well, it is a pertinent question. I'm working on a project for the Defense Science Board on dealing with the insider threat. And trying to manage the insider threat is such a difficult problem that we've just sort of casually speculated, you know, is it possible to conduct a war where you can't keep secrets? That may be an extreme concern, but nevertheless, it does reflect the fact that security is a very difficult problem. Most security specialists have now gotten away from the notion that you can somehow put a fence around your IT system and protect it. That's not going to work. There are some experiments with systems engineering, your IT system knowing that the bad guy is in there, and if he's in there, how can you stop him from exploiting his access? I think these are still in the domain of research advances in cryptologic technology, especially through quantum computing. It offers some basis for optimism that the computation problem can fix at least a good part of it by being able to encrypt the data. But there are necessary nodes between when data is encrypted and when it's not encrypted that still offer a vulnerability. So this is definitely a work in progress.

AUDIENCE MEMBER: [...]. When we think of the cloud, we're really thinking about those three datacenter instances. And even if we put them in secure military bases, most of those military bases rely on commercial water and power for those data centers to operate. And the typical military base only has about 14 days' supply of fuel. Is there any thought in the request for quote that would include hardening of the infrastructure itself?

SCHNEIDER: The question of infrastructure protection, not only cyber protection, but also physical protection, has been on the minds of the government for more than 20 years. There was a well-thought-out commission on infrastructure security in the late '90s that reviewed the problem. Initially, infrastructure industries were not particularly mindful of these problems, because they had many other difficulties. But more recently, they have become more and more mindful of the problem. And the electric

utility industry, for example, has done quite a few interesting things to improve the level of protection. But I think it's also correct to say that this is a very dynamic problem. The *Financial Times* had a very interesting story, about a month ago, about China's efforts to buy up the electric grid all over the Eurasian continent. And they observed last week that a secret Chinese buyer, through a British company, had bought control of the U.K. civil nuclear power industry. So there's many dimensions to the problem of the security of the infrastructure that needs to be engaged. And it probably needs, as DoD is trying to do now, to be engaged as a system, rather than dealing with the breaches, because the system has a problem, not just the individual elements of the infrastructure.

LINDBERG: Sir, you're next. Sir?

AUDIENCE MEMBER: Hi. The Pentagon has 500 cloud programs already under way. Army has its own cloud. Navy has its own cloud. Air Force has its own cloud. At the same time, as the government is completing JEDI, it's also completing a partner of a program called DEOS. It's completely separate. In light of that, wouldn't you say that the federal government or the Defense Department is well on its way to the multi-cloud approach that you're recommending?

SCHNEIDER: It's an interesting question, and how they'll manage it is to be determined. In DoD's response to the Congress, they discussed the issue of the fact that there were many other clouds – I think the figure referred to was about 500 experiments – which may make it easier to integrate the clouds. So I mentioned that we fight jointly, not separately. And the fact that the Navy would have a cloud doesn't assure that the Navy and the Air Force, for example, would be able to work together in a theater of operations. And so I think DoD is trying to find some way to harmonize this. And the fact that there is a fair amount of experience with clouds on a smaller scale, I think, may make it easier to have an integrated multi-cloud environment over time, as DoD gets past this pathfinder phase and looks at how they can manage the combination of importing civil sector best practices, improving security to meet the needs that the DoD has while capturing the innovation that's extant in this industry.

AUDIENCE MEMBER: Thanks for your presentation. I'm looking at the title; it's "Best Practices, Innovation And Security." The problem now is we have to look at that whole system, whether you are going to improve the productivity and the outcome. There's a dispute about how, who's going to be the winners – whether that is Amazon, or there's some other vendors, IBM or AT&T or whatever. Just wondering if there's some possibility that some major project would use a cloud, or some other small analysis. Maybe you don't need to be one centralized cloud until you reach the point, and then it's important to reach that point. A good result is that inside, the personnel and their productivity, current government agencies just don't have the productivity. And then other people are relegated negative productivity. And then they are not even capable of doing anything except maybe accumulate a lot of personnel to retaliate against good people. So I was just wondering if you can address these issues. How are they going to reform the government, especially DoD? They are still purchasing at a high price, low-quality merchandise? And so if you think about hacking, and it's not just Snowden, but also insider, they are still there. They are still there doing it against the general public and general employee. So I was just wondering if you can address those employees, staff and to improve their productivity.

LINDBERG: Thank you.

SCHNEIDER: The governance model is probably likely to evolve with the way in which the DoD adopts the cloud services model. And so I suspect there will be improvements. And one of the properties of this greater centralization, I think, it will provide DoD with much better visibility into the productivity and effectiveness of the components of DoD, because they will have all of the data, with the insights and on a continuous basis, because we're not only dealing with combat operations, but the acquisition system, the logistics system, the R&D system – all will be captured in this cloud environment which, by providing DoD management with insights into what's going on, I think DoD will have the opportunity to become much more efficient. And I believe many of the Industrial Age acquisition practices that now plague the productivity of the defense sector will be mitigated.

LINDBERG: Seth, do you think there's some hope for mitigating the problems of the Industrial Age acquisition process?

CROPSEY: The centralization issue here is divided, because, of the reasons that Bill has pointed out, at least security requires some kind of diversification of the cloud concept. But that's not what they're going for currently. They're going for putting everything in one cloud. So it sort of cuts two ways. I mean, the centralization issue is part of where and how we've gotten to where we are today, where things are increasingly centralized in the Office of the Secretary of Defense. And managing 150,000 employees turns out to be a difficult thing to do. So I think that the idea of cloud computing and of centralizing information is sensible. But the questions about security, efficiency and related ones that Bill raised are very much at the front.

LINDBERG: Sir?

AUDIENCE MEMBER: To Bill's presentation on the supply chain: is that threat a function of parts of components sourced from China, or could you elaborate on your statement?

SCHNEIDER: Well, there's been quite a bit written about supply chain contamination. And the aspiration that has been reflected, for example, in changes in the acquisition regulations that require the prime contractor to cascade down to their subcontractor certain cybersecurity requirements is a dimension of an aspiration to deliver uncompromised products to the end user. That may be utopian, in the sense that the opportunities for delivering uncompromised products face so many hurdles that some second-best solution may have to be found, such as systems engineering products to be able to cope with the inevitability of adversary penetration of these systems. But I think DoD is cognizant of the problem and will treat this as an issue. But my point in raising it in connection with the cloud is that the supply chain management has been easier when they're managing this supply chain for an aircraft carrier than it is for a cloud datacenter that will have tens or hundreds of thousands of computers operating in a virtualized environment, where the possibility of cyber intrusion is an important risk.

LINDBERG: In the back.

AUDIENCE MEMBER: Thanks. I had a quick question and a little bit of a follow-on in regards to the outcomes question that was asked earlier. In the context of when you look at this award down the road, where will we see in terms of how do we measure and communicate success? So in terms of the road that you went down of talking about centralized data repository, to be able to get analytics across the scope, do you see that in regards to where the RFP is today in regards to providing that data? There's not much, at least, that I'd read into it, and see whether or not you felt that was a part of it.

SCHNEIDER: Yeah, well, being able to extract insights from a government RFP is a difficult art, and I'm not sure I have a good grip on it. But I think the pathfinder concept offers some opportunity to find the points of friction in the implementation of the cloud. For example, from media reporting, I observed that the intelligence community encountered difficulty by certain agencies having problems. For example, the National Geospatial Intelligence Agency deals with a lot of imagery, or the National Reconnaissance Office, and imagery is notoriously more difficult to extract data, process and disseminate, compared to ordinary digital data that doesn't have these kind of complications. And so there turned out to be some points of friction. And I think that's the experience that has existed in the civil sector applications, where a cloud user, for example, would find that it was much easier to get a specific cloud service provider that would deal with document authentication and just let that cloud service provider handle the functionality associated with that, because they were experienced and able to adapt. And I think eventually, as we're starting to see with the intelligence community, the way they're bringing in a new team for different cloud services from Dell and Microsoft, that we may see this same kind of evolution in Defense. I think, as was noted earlier, the fact is that many elements of DoD have seen the value of the cloud, and they've gone out and used their appropriated funds to acquire cloud services. I think now, looking at DoD from an enterprise perspective, that they will encounter the fact that a single cloud service provider is unlikely to be able to provide the optimized portfolio functionality that DoD user will require.

AUDIENCE MEMBER: I want to build on something that you just mentioned, that you've mentioned a few times. You talked about this as a pathfinder. And I feel like, you know, granted I haven't read every single thing about this, but it seems like that's emerged more recently, like this hasn't always been described as a pathfinder. And I'm wondering why might it be the case that they would kind of rebrand this into a pathfinder project? And besides that change, are you observing any other changes that have taken place, given that they handed over leadership of this to somebody else completely, about a month or two ago?

SCHNEIDER: It's a good question. That's a challenge to your glasses prescription, to read the 33 pages of the industry and government dialogue and responding to the draft RFP. And it's clear there was a lot of bobbing and weaving on the part of the government. They recognize that the industry had some good points and a number of cases, at least as reflected in that document. The changes were made in the final RFP. This same document also suggests that a lot of things are still being left to the ingenuity, let's say, of the provider. And perhaps it reflects, as has been sort of an assumption of mine, that DoD as an enterprise is not yet a mature and sophisticated buyer of cloud services.

And so they want to see what the innovation the industry will tee up and see how it will work. I think the initial reaction to the draft RFP about the prospect of a 10-year sole source contract seemed to get – or did get – a very negative reaction from industry. The idea of a lock-in of a single provider was deterring to industry. And so the idea of the pathfinder, where the way that the firm-fixed price contract is constructed, so that DoD can get out of the relationship after a two-year period, even though if it was very successful could go as long as 10 years, it does suggest that DoD is looking for some running room to experiment and to arrive at a different conclusion, rather than go down exactly the same path that the intelligence community did, which now seems that they've recomputed, so to speak, and have decided that they want to move towards a multi-cloud environment.

LINDBERG: Could you just say a word or two about the role Congress has played in this?

SCHNEIDER: You know, part of the angst about the draft RFP did come from the Congress. Congress does have a default setting against sole-source contracts, even though the nature of the environment has at least in part been created by the Congress that has stimulated the need for sole-source contracts. But leaving that one aside, they still emphasize a basis to this idea of open competition. And the Congress did ultimately decide on a 15-percent withhold on authority to spend appropriated funds having...

LINDBERG: And what's that mean?

SCHNEIDER: Well, yes, that's a good question because it has a literal meaning, as far as what happens to the funding. But having done the stretch-for-one-year experience 10 times in the Congress, I can say that a 15-percent withhold is a speed bump. It's not a deterrent. And as a result, I think the executive concluded that they could describe their plans, which they did in the response of the Congress. And I thought it was well-written, and, given what the Congress did, it was a constructive response. And so I think the Congress, while they were part of the chorus about the angst on sole-source providers, they ultimately did not drive the outcome.

AUDIENCE MEMBER: What are the other key differences between the draft RFP you identified and the final one? And then, a follow up on that, as other government agencies look to cloud, do you think this contract is going to have an influence?

SCHNEIDER: Well, I'm not sure I have a line count there, because there was a lot of minutiae about renumbering the CLINs and things of that sort. But I think...

LINDBERG: The what?

SCHNEIDER: The Contract Line Item Number. Nevertheless, there were some important changes that were made in the final RFP. I think the notion of experimentation that is reflected in the pathfinder concept is an important one. It was emphasized both in the dialogue with industry, or at least can be derived from, as well as in the communication to the Congress that DoD is clearly experimenting with this. They want, at least for the initial volley, to leave the question of innovation to the cloud service offerors. And things, for example, like security: would they make having a cloud already qualified at a specific level of security a threshold for entrance? But it turns out that the way DoD manages it is that they would facilitate a qualification at higher levels, even if a cloud service provider currently did not have, say, access to top secret sensitive compartmented information levels of access. It begs the larger question of, will DoD find a way to climb the Everest of bureaucracy in trying to get security clearances for the people that have to work on this, in an environment where it takes about two years to get a Secret (SCI) clearance?

LINDBERG: Round 2.

AUDIENCE MEMBER: Having studied this procurement in depth, and having been an advocate 10 years ago of pushing DoD into commercial cloud, which I sometimes regret today, we see a couple false narratives. One is in the report to Congress. It said that a multi-cloud is too hard, and that the best practice is commercial single cloud. But we cannot find any data to support those statements. Also in their report to Congress, it said, because standards are required under the previous MDA called Modular Open Systems Architecture, you must embrace standards and open systems. And in the discussion around standards, there's no standards discussed. There are standards around cloud. And as we've seen in other monopolies that emerge in the market – and I won't name them all – they are going to fight standards, because if you're the first market player and the biggest market player, you don't want open systems because it creates competition. So we don't really have any reference to standards in this. And then we have justification for a single cloud based on false information. Does that not create protestable situations, when false information is being used to support a strategy?

SCHNEIDER: On that, the particular point about commercial practice, I think it was a bit of a dialogue of the deaf, because in the dialogue between industry and government on the questions, one of the industry questioners raised the issue based on commercial surveys of cloud use, and DoD expressed in this document that they didn't want to comment on third-party surveys. On the other hand, they emphasize the aspiration to be aligned with commercial practice. So I have, perhaps naively, fused these various data points of the pathfinder. The dependence on commercial service, and the willingness not to tell the commercial services or commercial offerors exactly how to do it, which is the default setting of DoD, that there may be a basis for optimism that the path DoD is taking will actually allow the commercial practices to dominate in the way in which commercial users actually set standards may in fact be the greater need. The tougher problem that DoD will face is, how do they adapt to commercial standards? How do they manage a security environment where they are comfortable with a system that is sclerotic and does not really depend on the kind of data use that would really make the system work effectively? So I think the environment is good. And I hope the industry will retain an interest in this, and help shape the governance model and the contracting model and the functionality that can be built into the system, so that the government can really benefit from this effort.

AUDIENCE MEMBER: Just to follow up on your earlier comment on a secure supply chain. In last year's NDAA, there was legislation...

LINDBERG: I'm sorry, the NDAA?

SCHNEIDER: National Defense Authorization Act.

LINDBERG: Thank you.

AUDIENCE MEMBER: ...Suggesting that requirement. And then DoD put out a publication, DoDI 5200.44, which talks about secure supply chain, down to the chip and component level. Is that a requirement, or is there any reference to that in this RFP?

SCHNEIDER: Well, that's an interesting question. They had a similar question raised about third-party software, and how do you do the verification and validation to ensure that the third-party software is not contaminated in some way? And they, again, left that one open as to how it would be done. There are commercial V&V processes out there, because commercial users have had similar concerns about the contamination of software. And DoD has actually developed a better system, I think, than the commercial users have for getting insights into counterfeit products and that sort of thing. So I think there's some opportunities for convergence, if the equities of commercial users have an intellectual property protection and so forth can be integrated into the way that DoD is doing it. But it's going to be, you know, *terra incognita* for both sides, in terms of trying to get something to constructively evolve.

LINDBERG: We're just about out of time, so Seth, do you have something on that?

CROPSEY: I wanted to ask Bill a question.

LINDBERG: It is permitted.

(LAUGHTER)

CROPSEY: Around the edge of this discussion today has been the question of the Defense Department's ability to adapt and to keep pace with the rapid change in technology as it applies particularly to information systems. If we were to fill up this room with Federal Acquisition Regulation books and the Defense Acquisition Regulation books, there would be no space left for any of us. Given that, and what you know – and what we know – about the Defense Department's speed in moving things that are important, are you confident that the questions can be resolved satisfactorily about speed, as far as weapons systems and platforms in the future? I mean, I think most people here are aware that the idea of modularity, and being able to add things in the future, is being built into systems. But is that enough?

SCHNEIDER: It's a very pertinent question. And even though I'm on here, at least in part as a former chairman of the Defense Science Board and a current member, I'd like to introduce a bit of sociology into this discussion. Namely, I think it's fair to say that it's very hard to get big, successful organizations to change. And the adaptation that the Defense Department is going to have to go through with a cloud is small beer compared to what they're about to go through with the almost complete inversion of DoD's – instead of their dependence on defense technology to produce defense products, they will be dependent on civil technology to produce defense products. And that will require a change in mindset that will be more difficult, I think, than the adaptation to the cloud, because the cloud is largely a civil sector invention, rather than a defense sector invention. So I think if you have an opportunity to interact with younger enlisted personnel, they are completely at-ease with cyber. The fact that they are digital natives is really a major change that's hard to account for in sort of objective terms. But just anecdotally, because we have such a young officer corps generally, I think the change will probably come a little more easily than we've come to expect, because at the end of the day, it's going to be the people wearing uniforms that are really going to drive these changes, and not the entrenched civil service with their 5,000 series tomes.

LINDBERG: Seth, you're riding up the elevator with the Secretary of Defense, and you have exactly that long to give him one piece of advice. What's your piece of advice?

CROPSEY: Change the model for the organization of the Defense Department of the United States from the Soviet one to one that looks more like an American one.

LINDBERG: Bill, same to you.

SCHNEIDER: Well, I think that because DoD has taken this step with respect to moving to the acquisition of cloud services, the subsequent steps are much shorter and probably less risky than the risk they've encountered by not moving to the cloud sooner. And so I suggest that they should move as rapidly as they can to absorption of the commercial model for the development of cloud services, and look to ways of adapting DoD needs, so that they can fit in to the greatest degree possible with the commercial model.

LINDBERG: Thank you, Seth. Thank you, Bill. Thank you, all.