

**Mr. Terry Halvorsen, DON CIO:** Ok good morning. I'd like to ask everybody to grab a seat. Well thank you for taking some time to talk with all of us this morning about the IT workforce and we can wander a little bit beyond that depending on what questions you might have. But I thought I'd start this morning with a little bit of discussion of where I think we are, what I think we know, and probably more important, what I think we don't know today about what has to happen with the IT workforce. In general, some of the IT workforce issues that are facing the government and the Department of Navy, but I'll talk a little about some of the concerns I have about the IT/Cyber workforce in general and where I think we've got to get some answers in a little bit better way ahead.

So obviously the first thing that concerns us about the IT workforce inside the DON is cost. And we've got to balance the cost of training the IT workforce, which we have to do and we are committed to, against the dollars that are available. No secret—there's going to be less dollars available to do some of the IT workforce training that we were doing. So you got a couple options: change the way you do it so that you eliminate some of the things you were doing. I think there are actually some places that we should do that but what we might have to do is replace it with a little higher bar. As an example, I do think in general some of the certifications that we have out now that we're paying for almost have to become assumed basics that the individual's got to bring to the table. We don't pay anymore. That could be anything from A plus to some of the Microsoft certs. I think they are becoming some prevalent and I'll be very candid, I'm also looking at what's the value to those. They are so proliferated one of my concerns is, have we potentially lowered the bar with the proliferation of all of the people that have that how we're delivering it. I don't know that that's true. I just am concerned, any time you do that with massive training that can be one of the things that happens. So that's an option we're going to have to look at. What do we do? What are the new standards? And how do we certify inside the government?

I will tell you one of the things that we are looking at hard is where does it make sense for us to self certify. Now people think we do that all the time. We self certify today in things like avionics, where we give the training, and we certify that it meets the standards and people go fly and fix airplanes. We have the highest safety rate of anybody who flies the number of aircraft hours that we do. We do that in many other areas. Is it time, and I will tell you I think it is, time for us to look at in the IT business, where we are going to do some self certification and pull that inside the government. I don't know specifically what we'll do yet. We're working on that, we're having some discussions and we'll also have to look at what's that leave for funding, what do we do with that.

I think the other thing that has to happen, and when we look at self certification, how far do we take that? What level do we say we're comfortable with self certification on? Does that run to basic network management? Does it include basic security? And then, some of the advanced pieces, we would say, ok, we want to keep the tie to commercial certifications. And we're looking through all of those options to include even in the commercial secto. One of the things I think we have to get a little better on, and there are some legal issues, contract issues that all would have to be worked, but I think we're starting

to get knowledgeable enough where when we say, hey we're going to go out for a bid, for example, for somebody to help us operate a network or provide security of a network, that we want to get much more specific about fine but if you're going to bring a workforce in to do that, we want a workforce that...here's the list. These are the minimums that you must bring, and much more specificity than we do today. I mean, we're getting better at that, but I think it's another area where we have to get better at saying, these are the things you have to bring to the table in terms of certified skill sets in the cyber and IT world.

The other thing is we may start requiring, I think in some places, and I say may because I will tell you there are lots—I will keep stressing that—there are lots of legal and acquisition hoops we have to go through and some economic analysis that we have to do, but I can see a point where we might say certain jobs in addition to specified certs are also going to have a change in, say, there is an education in general requirement, whether that's a full degree in an IT-related field, if it's an associate's degree, if it's something else, but we have to look at that. I think any field that truly is going to keep getting more professional has that as a requirement. I mean you see it...if you think about the fields that are very professional—engineering, medicine, and I think we're right in that—they have those type of education in addition to technical certification degrees. So I don't know the extent we'll move there but I think that's something we have to think about as we go forward with our workforce.

I would say we have concentrated a lot of our certs lately around security. I think that's good, but now I think we need to think about how do you expand that so while you're maintain the security focus what you really want to do is think about how do you more embed security from the beginning into systems which means you need your security person, your ops person, to be more integrated. Now, that could mean you have a security person and an ops person working together, complete integration would mean, you know, I take the two of them, cut them in half and put them together, we're looking at that in a biogenetics area down in Area 51. How that all works together, I don't know, but I do know that we've got to do that. I think embedding part of your ops so that security becomes just, in an ideal sense, and people always like to pull out your snippet quotes, so the quote will be "Halvorsen says security just becomes part of ops, lower the bar." That's not what I'm saying, what I'm saying is that security should become such a second nature embedded into what we do that it's naturally part of all operational pieces that we put together and I think in this business, we have to get there. It will change more rapidly and that has to be a part of our ops discussions. And it's got to be a part of what we look at as we evolve the workforce.

This is, I think, the cyber workforce, IT workforce, is going to be one of the most difficult to manage. And I think all of the people in this room should see why. If the rates of technology are changing and anyone here who thinks the rate of technology change is going to slow down doesn't belong in the room, that's just a fact, it's going to speed up. We might not be able to afford it all, but it's going to keep speeding up. So how do you take a workforce and at least get it as agile as you can in response to those technology changes, cultural changes, just the way we...you know, you'll get a program today say some system and we say hey this is perfect we're going to use this today to do general accounting of inventory. Then somebody looks at it and says, hey if you're accounting for inventory, we added this piece to it, we could also account for certain aspects of security. That'll keep evolving in addition to the

technology. How do we keep pace with that in the workforce. These are the things that I've spent a lot of time really thinking about. I think it will make or break us in the end, it will be about how the workforce gets us through some of the challenges. And when I say the workforce in that case, I am including the entire workforce and that means the contractors, the civilians, the military, everybody who's going to be a part of touching and operating our whole cyber environment and that's everybody. All the groups.

I also think there's going to have to be some discussions about what does it mean to be part of the cyber workforce fully integrated in an environment that includes military, civilian and contractors. One area that will impact us, and I will say this, people get upset, but it's a fact: we are way behind in the big category of cyber law and how that applies to everything—to acquisition, to managing your workforce, the laws haven't been written to govern an environment that will take this much collaboration, that changes this much quickly, that is frankly not an environment that has physical boundaries. We are in a virtual world. And we're not very good at writing the virtual rules yet. That's going to be...if I was investing today, as a side note, that might be something I would start looking at, what company is going to come together that starts looking at the policy rule sets in general, not just to the DON, but that are going to have to apply globally and certainly in our case federally across everybody. It's an area that we are going to be challenged in for a while. There's some interesting cyber rule sets. Fascinatingly enough, there are much better rules today written about audio and what's legal and what's not than there is about video and when you throw the combination of audio, video and all the data you can get from the cyber environment, there's almost no laws written that were written to encompass the whole spectrum you can bring to the table in the cyber/IT environment. That's going to have to be part of our workforce considerations. And I don't know how to do that yet, we're going to have to work for how we do that.

We are also going to have to look at how we get flexible in our workforce and still maintain frankly a cadre and bench strength of people that can react to financial changes, priority changes, that's going to happen in the cyber world too. We're going to have points of time where we're going to need to have just like we want, this is interesting to me in that if you draw the curve of what we want from equipment and it goes like this in cyberworld, you're going to need the same curve for people. That is an interesting challenge. How do you move up and down, draw down forces quickly, redistribute them to new priority areas, get the new skill sets in, old skill sets and equipment training out, how do you retrain quickly to the new skill sets? We're going to have that problem in the cyber workforce more so than, the only other place I think that is even close is the medical world, their technology is mirroring ours in the changes, it's the only other place that I have seen that is even close to having the scope of the problem we're going to have in the cyber workforce world. How do we react to that? I mean, I think—I'll do a quick comment, you can tell me...raise your hand if you know what I'm talking about. So when I say, we're going to take control of the horizontal, we're going to take control of the vertical, how many people know what TV show I'm referencing? Yeah ok, I figured that, you're all old, ok. And I can say that because I am old too. And Linda's hand didn't go up but I know it should have. Well they've heard the joke before and they know if they raise their hand they're old. But I think about what was the original training a lot of people in education that came into this business had. Watch the just sheer

volume of data, training and education that we need them to have and we expect coming in the door now with our entry level people. It's a fundamental and it's a huge change.

I expect today the entry workforce in this business to come in almost with everything all the people that raised their hands knew plus everything that's happened in the last 30 years. That's what they have to come to the table with. That's hard and that's going to continue to get harder. As we get more, in some ways, people say you're not getting more technical, devices are really easy to use. Got it. So here's the other big problem the cyber workforce is going to face. We make changes that make everything we do look easy. So I've had a career on the civilian side in two big areas: training and IT. And I will tell you, everybody above, actually I used to say everybody above the grade of lieutenant, but actually everybody who has completed any education thinks they know everything there is to know about IT and training. It's the two areas nobody has any problem giving you advice on how to operate them. Bar none, you go in and...we have become, some people have heard me say this before, IT has become like it or not and it's a testament to everybody in this room and all the things you've done, we're a utility. We are absolutely a utility.

I mean, no one comes in in the morning and some of you have heard me say this before, but you don't come in in the morning, flip the lights on, and say "God, that was impressive, I have electric." That's really cool. You come in in the morning and that one morning that the light doesn't come on you go ballistic, "What the hell is the electric company doing today?" We're at the same point now in basic IT services. No one comes in anymore and marvels at, "Hey, I'm actually at this IT system that lets me connect with people in Europe, I can do email, I can do file storage, instant communication..." No one marvels at that anymore, that's the expected, utility level of service. Those expectations get higher, now we want to be able to click and do video on the desk, share my power point, talk in four different conversations simultaneously, and do that without having to train any of the end users. So what does that mean about the workforce? Well, to do that, that means behind the scenes, we're all running frantically. And we are, and we're learning how to do that in many cases about the same time we're fielding it. That's a much more demanding environment to be in. You've made it look easy, and I have been in this conversations at a very senior level where people say, "Well what do you mean you need some money to do this, that's so easy! I go right to my desktop, I click and I get video, how hard can this be?" Well it's a little harder than you clicking right on there. I'm thinking of having someone, this might be a contract we put out, to develop a video computer interface that when you click on that video, the first thing that comes up is all of the things in a movie, a 50 second movie, that had to happen for you to be able to talk at the other end of that video. I'm thinking that might be, we may just do that for marketing, I think it will be a really powerful tool. But we're going to face that battle, we are already facing that battle. It is not a secret, can we turn that projector off, we don't need it. It's a room full of IT's this should be easy. Perfect, thank you.

How we balance that, where there is already a piece that says ok IT should take more money out because they're easy. And oh by the way, with IT we're going to save money with travel, we're going to save money in file storage, we're going to save money but we're going to take money out of all the things that empower me. That is the equation we're faced with today, how to do that. So we've got some education to do, part of cyber workforce's role is going to be, and I don't know any other cleaner

way to say that we got to figure out how cyber workforce people also have a skill set in marketing, and it's really more than that, it's a skill set in being able to talk to what you do in terms that everyone can understand. Now, please don't take this the wrong way, that's not a skill set that as a group we're very good at. Most professional groups aren't, we talk in our own language. I just had a demo with, I'll tell you, it's with Microsoft own link (18:51??), and the opening dialogue, the guy's telling me all the things that are happening, contained only four actual English words. Now I knew perfectly what he said, anybody who was not a part of business that would have looked at it like, "What??" and we face that all the time. So one of the things I'm going to urge every member inside and outside of the cyber workforce to do is work on your communication skills in how to explain what you do to the rest of the world.

And here's another thing that hasn't disappeared, and I'm going to tell you as a group, we are terrible at this, and everybody keeps saying this skill set is dead. And I argue that not only is it not dead, it's become more important and that's how to write. One of the things that if I have anything to do with it, we are going to mandate into, and I said the word mandate for a purpose, we are going to have in our cyber workforce training, some written requirements. And have some bar about how to write, because I'm going to tell you, most of us don't write and we don't write very well and people say, "Well I don't need to write, I do email." That's how you figure that one out. Well I do chat. Well everything I do is in a power point brief. That's right, it is a different style of writing than writing a formal letter, it's actually harder to write in that style, be more concise, and get your key points done. So what general happens is when we have that conversation, we get to writing, you get seven or eight pages of email that miss the point. That the customer wants to get to and the commander, I'll use that term interchangeably here because we write for two audiences, there are customers, there are commanders, but they both want the same thing. They want to read the least amount of words possible to get to the bottom line to help them make a decision. That's what they want, that's the value statement. We're not good at that. We have to get better. It is how you get more. It's how you protect money. It's how you explain what you're doing when you say, I'm going to spend more on IT to save you more money here. So that's my lead in to the next thing the cyber workforces have to work on.

Last 18 months, we very much focused inside the DON on how to take money out of our business IT systems. Not a secret, we are over the FYDP, inside the DON, taking \$2 billion out of systems that are predominantly business oriented, they're not tactical operations systems. We're going to continue that, but the focus and I got to be careful when I say this, we're not going to lose focus on that \$2 billion. I have a very personal interest in that, I will share with you, I have really one objective from...every year we have to do these senior executive objective statements. Mine is a little easier because I only work for really two people. I work for the under and the SECNAV and they're not keen maybe into following all the elaborate objective systems, so SECNAV was very clear, he says, you have one prime objective, get the \$2 billion, you get to \$2 billion, things are good, you don't get to \$2 billion, I won't worry about you anymore.

So that's one of our objects, but my second objective now is how do you transform IT business and related processes to save more money in other areas. So how does IT enable, truly enable us to take money out of other parts of the business, other budget lines? How do we say, ok if I made an

investment here in IT, and you're going to hear me keep saying, and I change some corresponding processes, because I am convinced, single changes in IT the systems rarely produce what they promise. Till you've also looked at the business processes that you are impacting and make sure that they have also changed along with the IT, you don't get the total savings. Now people will tell you, no that's not true, these IT systems by themselves can save you money. I rarely see that to the extent that I need to save money. And it rarely meets the promise when people come in and tell me, hey if you put this IT system in, we're going to save you \$30 million. Generally that doesn't happen and the places that it has happened, it has been where we spent time with the business process we were changing and modified the process or modified in our case the hard part is modified the processes with many pulls. So one of the other things I think that the IT workforce is going to have to have some skill set in is understanding other business processes. Or at least understanding how to map them and understand how they integrate and actually yield to production in your IT system. You're going to have to understand that.

We have and we were faced in the DON with IT systems that when you first look at them and people do this particularly people who count money, look and say, well you should be able to eliminate all these systems. They're all basically doing logistics. Well, because of the way we grew up, there's no foul in that, that's how most places grow up, what you find is the business processes around each of those logistics systems are different. Sometimes they're different in a fundamental way that when you absolutely analyze the process, you come back and say, you know what, no, it doesn't make sense to change this or try to force it into a different system. But probably 50% of the time, what you find is that the process change can be made and you could get to a simpler IT system that would save money, but you've got to go back to that business owner and say, you are going to have to change part of your process. And the other hard part is going to be, you're going to go to another business owner and say, you five over here, your process can stay the same, you're in the system we're choosing, you're good and you don't have to spend any more money. You five over here, not only are we going to change your IT system, but you have a process bill, cough it up. That is hard in our current construct to do. Frankly, it's hard in industry's construct to do in most cases too because I've heard from industry leaders as they have tried to work that. But it is something the IT workforce, we are going to need to understand. Parts of it are, how does that business connection work? I don't know who said it yesterday, but I thought it was a very profound statement.

I do not think we understand to really any high degree how integrated and linked all of the processes and the IT systems are today. There's one of those commercials out on TV that says, you know, what does growing silk in China have to do with the price of milk in Ireland and shipping hazelnuts to Colombia. And the company goes and says, we can tell you all that. A) I don't believe they can tell you all that, but I get their point. We don't know all of those connections. It is something we're going to have to take some time to do, because as we change these processes, there will be second, third, fourth order effects that we will have to understand, and we're going to have to get good at that so we can change the processes and simplify the IT environment inside of the DON. And we will need a workforce that can look at all aspects of that.

And some of that is going to have to be inside the IT workforce. Does that mean I can't work with accountants? No, but you got to know how to talk to them. You know, many of you know, the

Department of Navy as the whole DOD, Department of Navy, we are on a goal now to be financial audited. SEVNAV has said, we're going to do that. Part of our initial discussions with that has been very interesting so you'll have the finance guide come in and they'll say, hey, we need you to demonstrate that your system is secure and your data is certifiable. They had that discussion, I said, well that's easy, here, my systems are secure and certifiable. Oh no, that's not what we really meant. See your definitions today on IT secure and certifiable aren't aligned with the financial IT definitions of secure and certifiable. They're different. Got to be able to have that dialogue, and we got to understand those differences.

And the last thing, and then I promise to shut up, that the IT workforce is going to have to understand, and I don't know really how to say this, so I'm open to changes that were done, I'm going to say, we got to understand data structure, data definition and data standardization. I was with somebody this morning who actually used part of that around, you know, for a long time we went on a big ABC accounting binge. We were going to take that all the way down to I think it's the 10<sup>th</sup> level of the temple on ABC accounting that you have to get. And then somebody got smart and said, you know what, after the fourth level, all your savings are gone. There may not be a big reason to go there. That's an oversimplified statement but we are going to wrestle with that part about what is data standardization, what level does it go. When I had a discussion yesterday about do I need to have a DON data definition board, where's Dave is he here? Dave Greene, done a lot of thought on this thankfully, about architecture and data definition, we are going to have to figure out what does that mean. IT workforce is going to be involved in that.

The industry, and I've spent time with industry leaders who went on kind of a complete data standardization, data modeling, data definition binge, and they spent millions of dollars and they have absolutely zero to show for it. We can't afford that mistake. So what are we going to do? But we are going to need to do that. If you're going to...I want to talk a little bit about this enterprise resource process, not ERP the program, I just want to talk about the process. If you do a lot of reading on the process, one of the things that becomes clear, the companies that did that successfully, and the good news is there's not a lot of them you have to go read at, the volume of data on successful ERPs is much smaller than the volume of data on unsuccessful ERPs. But one of the keys to success on that was having standardized data definitions on things you might not have thought about. So one we talked about yesterday is define dining facility for me. What is a dining facility? Well if you don't have an agreed upon definition of what that is, or pick another business unit, anything you want, if everybody who's in the ERP hasn't used that definition the exact same way, reported it the same way, when you roll it up for the decision to the decision maker, you don't have the right data, you tend to actually make some pretty bad decisions. How do we work through that? That's just one example.

Personnel business, Scott's here. I know that they are wrestling with it and we're at a tension point that I keep telling him you got to do your processes faster and Scott's saying but I got to get them done and he's right—he does have to get them done faster though. He's got to come to us with an environment where all those personnel definitions are not only standardized, but he knows where he's getting them from. Where's he getting social security data from? Where is he getting authoritative pay data from that's going to report? And we didn't grow up in a system that put them in one process or one IT

system. How do we get there? So data structuring, data defining, how do you store data? And I don't mean the physical data storage. How do you store it in a way that's retrievable and it's retrievable in a way that everybody actually knew the definition you were retrieving it by. Hard things that we're going to wrestle with in the cyber workforce. So that's kind of the challenges. I know I didn't tell you a lot of answers today. Don't have them. We're going to work hard on this, we're working to figure out how we bring industry in to part of those discussions in an open partnership way. We've got some questions out to the legal team, because I think I have to do that, I think getting...I want industry sitting right in the panels that help us decide what our cyber workforce is going to be. Because I think this is another place where we've really got to parallel all the things we just said about data standardization, that's got to be the same when we talk about our industry partner workforce, we got to know they're the same train, they've got the same understandings that we have internal, or we'll talk past each other and we do a lot of that today.

Questions? Sir, do we have a mic or anything?

**Audience member:** *I'm an MBA student...and in one of my graduate classes entitled cyber law and legal issues I wrote a research paper. My research paper was titled "Cyber espionage warfare"...my thesis for that paper was there are no networks in the United States that are 100% secure. And I went on to describe that, and by the way I know how to write and I'm an IT professional as well.*

**Mr. Halvorsen:** Good!

**Audience member:** *In my paper, I described from the time the Internet was commissioned available to present day, so significant events that cause us to be vulnerable, such as the federal reserve bank in Cleveland being hacked...which the United States caught. And other incidents that were both military and private sector related and I also stated the weakest link is people/consumers. In other words, we learn what not to do, but as consumers we buy the products that are just as vulnerable that we're trying to protect an employer we work for. So my question knowing that, for example our smart phones, carrier IQ that allows keystrokes of everything that we type into our smart phones, but the employer legally can't control that because as consumers that is my personal smart phone. But it's a residual risk, not only to the employer but also to the Navy, Marine Corps and Department of Defense. My question to you, sir, knowing that and knowing what these technologies bring, we live in a click, record, post it world. There's going to be "I got you"s that are out there. There's not just at your level in Washington DC, it's going to have to be at the ground level...San Diego...there's going to be events that occur that are negative. Because we're consumers, so could you address how you would envision to try to address that knowing that you're legally constrained from...?*

**Mr. Halvorsen:** I want to start with a couple, and some of this will seem, and some of you know me, I tend to be a little sarcastic, when did paper become 100% secure? It's not. But I understand the risks better. In its simplest form, what we've got to be able to do is understand the risk of the new environment better, the mitigations and the risks taken. Now why does the consumer buy those products that you just talked about rather than something else? There's a really simple answer, what is it? Price, they're cheaper! We're going to buy what meets our requirement in the best way as a

consumer. We do as consumers our own risk/cost analysis. We may not do it very well, but we absolutely execute. And we say, you know what, I'm going to buy this iPhone and I'm going to use it even though I have some understanding of what the risk might be, I'm still going to use it. We're not going to stop that. We are not going to stop that. So any technique that says we're going to stop consumers from buying those is not going to work. Now you said something, legally you can't control that. One advantage that we do have in the environment I work in is I can control some things. You can go buy that iPhone, you just probably aren't using it in any environment I control. You are not going to be able to even have it on in some environments I control. So if you want to be able to do your email and your personal email together, you're going to use the device that I say you're going to use or you don't get it. That is one way we'll have to get a little better at control.

That only will last for a little while, because we are consumer based in IT and that's going to continue to drive us because it's going to drive our costs. So we are going to have to figure out how we work better with industry, how we better partner, and understand some of the things that industry needs to protect. We're I don't think good at that yet. We have dialogue with companies and we'll say, ok you want to come on great, give us everything you know about your product, let us put all kinds of stuff on it and then you can come in. Well, I try to put myself in reverse, if a company came to me and said, ok DON CIO, we want your product, and oh by the way, to get that, we want to know everything you have, technically where you store it and all that stuff, would I do that? No. I wouldn't. And I don't, it's the exact reverse, I don't do that. How do we partner and we are going to have to, this is another place where I will say see point 1, the law that governs this is almost completely absent. There's not much, we're interpreting laws that were written for what I'll call a more hard environment, paper, Xerox, we're past that and that law hasn't caught up yet, so we got to look at the law.

We do have to educate people better about the risk analysis that they make. Do I make phone calls on an iPhone? Yes. I have one son that still has one. I won't say that he's the slower child, but maybe he is, I don't know. The other son got rid of his iPhone. Do I do banking on the iPhone? No I do not. I don't do banking on wireless either, which makes me a little primitive, a lot of people say it's secure, it probably is. Personally, I don't do any of my banking on wireless. I don't have that much money that if I lose any, I would be in bad shape so I do all my banking on hard site with encryption. But that's a personal risk statement and we'll have to educate people I think how to do that. Inside the government, in our systems, we have to continue that education. We made some pretty good strides a couple years ago with really pushing education of all of the sailors, soldiers, civilians, Marines, everybody about what they do. Frankly, in some years we've backed off a little bit with that, what's happening? We're seeing some of the same mistakes we thought we'd fixed come back. You can't let that stop. It is going to be constant education. The turnover in the business, we could have told us that, particularly with the sailors and marines, they're not in this for life most of them. So you're going to have a turnover. We bring in between the marines and the navy, I think we're bringing in each year about 42,000 new people into our company, just on the military side every year. So they're all going to be the ways we have to mitigate that. What's the next question?

See I knew if I answered that one long enough, nobody would ask another question.

**Audience member:** *Sir, I was appreciating what you were saying earlier in the presentation about the certification emphasis on the security as well as trying to get the ops people involved in that now. My question to you is a couple different things, but basically, are you also going to anticipate furthering the management and oversight supervisory folks that are not related to security specifically but are related to IT into the certification and credentialing processes specifically in regard to the 22-10 series and are we going to see things such as actual issuances of letters of appointments things like that and possibly an updated career guide in regard to that?*

**Mr. Halvorsen:** Ok so I think you asked me three separate questions there. Are we going to bring in the full scope of the personnel and organizations that need to be involved in making security inherently part of our processes and embedding it? The answer is yes, you have to. Then you asked me another question, says, now does that mean we're going to certify and I'm assuming what you're implying there is that are we going to give letters of appointment to people outside of that area that can then certify security? I don't know. I don't know. I mean, I wrestle with that a lot. There's a part of you that says...part of me says you should, I will tell you this, when we do that, and it may be in the execution and I'm willing to believe that, we haven't had good maintenance of the standards. So that could be in the way we execute, could allow a change in the standards, but that's something we're going to have to think hard about. And it's something that the operator owns the decision on. I actually think, and one of the things we're going to have to figure out here, is how in this new integrated cyber/IT, how do the operators play in some ways a bigger role, I would also say a more informed role, about all of the aspects of IT than they currently do.

Here's what I'm going to tell you, on the acquisition side, when you talk about managing a contract, they have multiple letters of appointment. Maybe they don't have the one that you want, but having spent many hours with them, they have multiple letters of appointment. We've talked about and one of the things that I'll have a session on that some of the Mags Coms and S2s (44:10??) with the Navy and the Marine Corps today is do we need to look at how we certify command information officers? Don't know that we'll go that route, but think it's a discussion. I think it relates to the discussion I had earlier about if we're going to be a truly professional force, there's got to be some level of certification, education, training that we expect and have to be part of those positions. Now we're a new workforce in a new area skill. We did not start with the first medical doctor having all of the standards in place that are there today. That also had to grow up, what do you do? We're going to have some of those same growing pains. We're going to have to grow faster in that and have our understanding mature to a higher level, but we're going to go through some of that. What does it mean? And that's a discussion that inside the DON we're going to have to have with the services at all levels so that they're involved in that because there are implications to all that, like second, third, fourth degree, we'll have to understand. But we got to do something in that area. Might initially be something sort of short of a certification, maybe it's an appointment letter, I don't know, but something like that I do believe we've got to get to.

**Audience member:** *Sir I have two questions for you. One is your thoughts on cloud computing and going to the cloud and then not going to the cloud. And then the second part is server consolidating using SPAWAR, DISA and the cost associated with that. I'm at a lower level facility, I'm with Bethesda*

*Maryland Surface Warfare Center, Carderock Division, so those kinds of things really impact our day to day business.*

**Mr. Halvorsen:** On going to the cloud, not going to the cloud, yes. That's the answer. That is the answer. Yes we will and in some cases, no we won't. And we'll go to the cloud, and I'm going to say the same thing for data center consolidation, we will go to the cloud and use it when it's best value, meaning that it's secure, costs me less and provides the same service, we're already in the cloud. I think that's a point..we are already in the cloud. What I think we're going to have to do now is look at where that makes sense to expand and here's where I think the areas that you might look at cloud. When you have a large concentration of similar services, it might make good economic and operation sense to go to the cloud. So no secret, a big bulk of users inside the Department of the Navy are what I call, and when I say office workers, I don't mean they work in an office, but they work around products that are like Microsoft Office, that's what they use. It doesn't have to be Microsoft, but the fact is today, we are a Microsoft Environment, that's just a fact, it's no guarantee that we'll stay there so all of you are thinking that Halvorsen said Microsoft is going to be the environment, that's not what I said. What I said is, we are today in a Microsoft environment and we have works who work around an office environment. To a real high degree.

It might make sense for us to look at an environment that puts all of that in a cloud and you go and pull it down as you need it. The advantages to that are I can then have a much thinner client, now I didn't say thin client, I said thinner client. It could reach at some point a zero client, for some users, it could be a traditional thin client for some users and it could be something that hasn't gone on a good fitness program and hasn't lost all the weight it needs to yet client. We're going to have all of that inside the DON for a while. How we manage that, where we apply that, is going to be based on operational security and dollars and the risk balance across all of those so that's how we would use the cloud. Data center consolidation is enabled to a higher degree if we figure out how to share that data and those applications in a cloud. We are going to have to look at, and one of the things that we are getting more mature on and industry went through this and they're still going, there's data center consolidation, you can call that data standards and data definitions, that could be defined as, I'm just moving data into servers.

Now a whole bunch of you will say, that doesn't save any money. It does save money. Every time I take a facility off line I save money. It might not be IT money, but I save money. I don't save the maximum amount of money I could in a data center, but I save some money. The second part of that is you include in your data center consolidation application rationalization. Everybody says, you're mincing words, you say application rationalization, you mean application reduction. No I do not. I, yes, will reduce some applications, but some of them I really do have to rationalize. Rationalize can be defined, again back to that data example, I modernize the app, I merge it with another app, I take it and make it a more off-the-shelf app. Those are all things that help us do data center, and when we do...why are we doing data center consolidation? Just because the fun of consolidating data? Save money and produce a better operating environment so all the things you're talking about have to be done somewhat in alignment. Now you are going to have to pick and choose, and that's what we're having to do, where we push the alignment button. Right now, in some cases, on data center, we're pushing the alignment

button around money. Got to get some money quickly out of the system. It is a lower risk way to take some money out of the system. Second phase of this will be more about how do you drop applications off of that, how you rationalize the applications, how do you maybe even position the data differently so you don't even need the storage we currently have? So what do you think is one of the big storage requirements in the Department of the Navy, what drives it? Certain thing that all of us use, guaranteed. Drives storage requirements. Email. Email in general. Again, we are today, so your answer's correct, it's changed, Microsoft based, but it wouldn't matter what you were using in terms of email.

Email has a higher overhead than other forms that you could use to communicate. It has a higher overhead than say chat and IM. Maybe you have to look at the ways you're communicating. Now for those of you who have read it, there's a couple places in Europe, a couple companies that have banned email. They've knocked it off. They've found that if they provided their employees an IM environment, it worked more effectively and they just eliminated corporate email. Now, we are not, I know somebody's back there writing, Halvorsen says we're going to eliminate email. That's great, we're not going to eliminate email. But what I tell you is, so 10 years ago, how many of you lived on email? 20 years ago how many of you lived on email? So do I think 10 years from now, we'll be living on email? No I don't. I do not think 10 years from now we will be living on email. I actually think less than 5 we won't be living on email. We'll have it, but we won't be living on it.

Our communication percentages will shift to something else and it probably initially will be a combination of something like chat and something like IM that's not either of those things either. So we're going to have to wrestle with how do we do that, where is that best done. It's happened in some small places. Where it hasn't happened yet is what I would call the mega corporations, there's not a single mega corporation that's not still doing email. We are a mega corporation. We're like fortune 2 if you put us all together. And you could argue, and I do, that we're actually fortune 1, it depends. And if you add the army in there, maybe we're fortune 2, but who knows, by the end of the FYDP, we may be fortune 1. That was a joke. We're going to have to look at how we address those issues and the cloud is one answer. There are other answers to that, but you have to look at them all. And here's the thing that I think we all get wrapped up in, whatever answer we choose today, one of the things we have a problem with and it's we at every level, so we choose today to say we're going to do data center and applications this way, whatever way that is, partly in the cloud, partly with thick. In our environment, particularly in our environment, we've gotten flexible enough to say, you know what, the decision we made 18 months ago is no longer the right decision. You got to change it based on technology, dollars, ambition, all of those things will impact what we move forward on. We are not yet agile in our own thought processes in how we make decisions to do that, this is an area we'll have to focus on here. Next question.

**Audience member:** *Morning sir. Speaking to the self-certification, wouldn't it be better instead to go to a central funded certification school like MIDI underneath the LEA or something like that rather than spending up our own program which quite frankly I fear would become outdated because it takes so long to change training formulas?*

**Mr. Halvorsen:** Yes. No. Could be. You kind of made the point. So when I say self certify, I don't know that I need to change anything I do today. We have on both services for the last 2-3 years greatly increased and improved the amount of knowledge and skill set that everything from the Navy A-school to the Marine Corps basic guys coming out, they know more today. I don't know that I need to do some of the certs that we were saying they had to do after their new age schools. I think that can stop. No change. I think we've already built that in. I think there's a place to say you might want some of the advanced skills centered around a central place. Now here's where you go into problems. You say a central place. I am not an acquisition person and people who know me would tell you I am not always maybe the biggest champion of acquisition processes. But I am coming to believe one really big thing. If there is no competition, you get no value. If you lump it all and say, you have no become, David here, has become my single provider for almost anything, quickly he will become less value. That just happens, I don't know why. It will happen. So I think there's a point that competition has to play, and that doesn't mean competition always in the business sector. It can be competition inside the government, so you might say ok, DISA is going to do this piece, War College is going to do this piece. And oh by the way, I'm going to recompetete that internally every two years. These are the kind of things I think we have to think about in this business more so than maybe some of the other places where we train because of the rate of change.

The only thing I'll comment on that, better handled by the acquisition, do I think that the timeline on the acquisitions is driven by the rates of all type of change inside the cyber/IT environment? I absolutely think that was a factor and I think you'd almost have to say yes. Is it the only factor? I don't think so but there's probably enough acquisition people here today that after this you could ask them that question.

**Audience member:** *Speaking of the IT workforce, we have the telecommunications side they do the 391 type stuff, we have the 22-10s and their various parenthetical, when it comes time to try to find someone who has an appropriate skill set and there's no degree requirement with the 22-10, so I'm going to go on ahead and grab an A-54, but the A-54 computer engineer is thinking inside of his box instead of across the architecture. Are we going to do anything to professionalize if you will between the two...?*

**Mr. Halvorsen:** Dave the answer is are we ... and I want to answer it this way ... are we going to do stuff to professionalize the cyber/IT workforce in general? Yes. Now, what I think that means is, I think we got to redefine a little bit the whole way we label the skill sets. I don't know anymore the definition of you're a 22-10, you're an 802, you're a workforce... I mean here's the, the demo that I took this morning integrated every aspect of comms. What we are talking about here in the IT workforce is an aspect of communications, it integrated every piece. It was IT, it was telephone dial up, it was video, it was email, chat, it was a system that integrated all of that. Well, if you took our current model and you tried to build how would you man that, I end up with 26 people. Just if I mapped it by the skill sets required to do that, that's not going to work, that won't scale. So what is...I think we're finally going to have to really address what is the right set of skills, how do we blend them and mix them? And some of the nomenclature we have today may not hold. In the interim step, we're going to have to figure out how we take the current structure, make it work better, in that case we might have to professionalize the 22-10 more but the longer gain is what is the right structure and how do you really take identifiable skill sets and mix and match them how you require them in an ever-changing environment.

**Audience member:** *The biggest problem we keep running in to is that the computer engineer will think inside his box, the computer scientist or 15-50, he doesn't really care about layer 3 or anything below that, and then you got your communications guy going yeah your circuits out, it's good, and so forth. But to bring it together, that's where I'm thinking in the 22 series we have 10 parentheses and none of those have a degree requirement. We need to start looking at that as far as...*

**Mr. Halvorsen:** Yes we absolutely do. We have to look at that and I think what we may be talking about at least in the interim is, whether it's a 22-10 series or a new series, it's...I'd just like to call them integration guy. Or integration girl. But it is that person who can actually think, and I love to be able to say this, outside the box. The box being the hardware that's either on your desk or the virtual hardware that we're positioning on your desk, can go outside that box, can go into the communications circuit pathways that you have to be able to talk about to make all this work. And who, when we say troubleshoot, anybody who's worked in this business knows there's a trouble shooting issue, so I used to love this, Lynda and I had this discussion in my last job sometimes. So you call up, the circuits down, you call the circuit guy, circuit guy says my circuit is perfect, I've tested it. Ok well it must be then the box, my box is perfect, I've tested it. Software, my software is running perfect, I've tested it. So then you ask him, well has anyone tested it all together. That's not my job. And it isn't, but somehow it's got to be somebody's job who understands and you'll hear me get off on this, and I promise not to go on a rant about this, but that deals with, I simplify by calling it network complexity. I don't mean network in the terms of a physical network, I mean network in terms of all of this has to work together to get what you want. And we are very much have to do some work to eliminate some network complexity issues, or we will lose this battle.

**Audience member:** *I had a question with respect to what is the Navy's definition of the cloud?*

**Mr. Halvorsen:** Good question. I'm not answering it, it's a good question. I don't know yet. We have working definition, the Marine Corps has a definition, the Navy has a definition kind of working with DON, but why I dodge that right now, what's industry standard definition of the cloud? There isn't one. Well that's one definition of the cloud. I bet you I have four or five other partners here who would argue with that. I don't know that we know, and I don't know that right now, that is important to define singularly the cloud. I think we do have to define those things we are talking about putting in the cloud in some definition that we all can agree on. Doesn't even have to be 100% right at first, and it will change, and that's what we're trying to do today is work on, cloud at the top line and then four subparagraphs to say, these are the four types of clouds or integrated pathways clouds we are going to define beside the DON partnering with industry having to do that.

*(Inaudible question)*

**Mr. Halvorsen:** So the question is: how are we going to use social networking, social media, how do we exploit it better? Social networking and social media frankly is just beginning to emerge in the business sector. People tell me, well Facebook is a business and it uses social media, it does but it doesn't use it in a business model, it uses it in a consumer model. The biggest social media deployments they are around

a social model not a business model. There's a big difference. In a social model, I don't have all of the requirements both legal and operational that I have in a business model.

One of the things you wrestle with if you use a social media environment, there's not a way right now to capture the data that you're legally required to capture. You got to work there. In a business model, I absolutely want to control part of my message. That's a fact. Hard to do that in a pure social media model. As that emerges in a business social media model, we'll take more advantage of it, I do not think, I don't think, the DON or DOD will be on the leading edge of that as it becomes into the business world. I think that's one where we will wait and see how it develops, it's approve an enterprise business model, and then we will began to move into that more fully. Now, not to say, because I do see the quote, "Halvorsen says Department of Navy not in social media." We are absolutely today in social media.

Anybody here from recruiting? Scott is heavily into social media and Facebook in the recruiting. Why? Because he wants to reach those consumers, so the consumer model works and Scott has put in place structures that protect the data. It probably takes more of Scott's time than he would like to think about how he makes that all work and comply with all the things that we have laid on top of him to comply with. But it is not yet into the mainstream business model yet. There are some softwares that are coming out and I think the first place that's going to be exploited is in terms of data collection, analysis and integrity. And maybe even message control. There's some new software coming out that have just started penetrating some what I would call classic businesses. Some places in the insurance business, where they are fielding their local websites but using a social media enhanced software that frankly monitors what all the local sites are doing, making sure that the baseline message that that company wants out there is protected. It can be distributed in different ways that appeal to each local area but they have complete control over the base message. They're analyzing their policy sales using social media data which they can do. Now the other issue you run into us in social media, you think about some of the things we might want to analyze out of social media and then I'm back to the point I made that there's some walls that have to catch up to how you would do that and do you really want to. People doing that, it's two questions we haven't really answered well yet.