

DON IT Conference, West Coast 2014
CIO Town Hall, Feb. 12

All right well good morning everyone, thank you for taking some time to come see the CIO panel forum. We've got a good panel, as you can see. Vice Admiral Branch from the Deputy DON CIO for the Navy, Janice Haith, who is kind of the functional lead day to day, and Robin Thomas from C4, and I would say we gained when we traded Robin for Kevin [Nally].

This is an open forum; we'll take questions that are centered around the topic. I'll just tell you this, most of you have been in discussions like this one with this group, and the environment that we're in has not changed much. We are still facing huge financial issues. I've had people ask me while I've been out here, "Well didn't the sequestration fix that?" I'll try to put this into some numbers terms. Before sequestration, and we were looking at the whole picture we had this much money. Then when sequestration hit we were 50 billion dollars short, and it provided some relief. Now we are only about 39 billion dollars short. So you ask yourself if that helped a big deal. It helped, but we are still under great financial pressure. If you're reading some of the tea leaves I think that you will see that financial pressure will increase. I do not think we are done yet with the cuts that we will have to take, particularly in the out years as we balance the requirements we have for defense against some of the more domestic requirements that Congress and the administration are facing.

We made some specific policy announcements, from DON, the Marine Corps, and the Navy. We are happy to take questions on that and where we are going. We are still about saving the dollars and our prime objective is to be able to take money in areas where we can take risks. We are much more comfortable taking risks on the business side and putting that money into the operational and tactical pieces.

You've heard from some of our senior leaders that there are some gaps we have to fill. The gaps have to be filled by moving money that was originally going to do something else. Part of our job is to help leadership decide where to find that money. We also have even more robust efforts to try to determine and be able to show where IT is an enabler, and when they go to look at the budget money shouldn't be coming out of the IT budget but out of where the actual savings is occurring.

The other thing we're working hard on is IT transparency; we've got to be able to show the IT money better. Some would say there is a risk to that, but I think if we can show what we are doing the gain outweighs that risk. I have to put one plug in because I got a note from Secretary Rayburn this morning, and just want to let everyone know that inside the DON we are pressing forward with clean audit statements. You will hear a lot about '17, but the bigger issue is beyond '17. In '18 and '19 we need to have auditable at any time systems. That's a much harder task than to get to a one time audit in '17. The DON is committed that we are going to get to a clean audit, so IT plays a huge role in that. We have to look at how the IT systems now must be auditable by commercial standards. So we will be working that, but at some point I think we will need some industry help with that. I'll turn it over to Adm. Branch now.

Adm. Ted Branch: Good morning. I'll make just a couple of remarks. My name is Ted Branch and I see only a few familiar faces out in the audience, and you all are probably wondering who is this guy up there with all the people who do the real IT work. I've been on the job for about six months, and I've got about an inch deep and a mile wide of knowledge. You can ask me any question you want, and if I know the answer I'll tell you, but if I don't I'll give it to Janice or Terry. But I'm happy to be here and engage with you this morning.

IT governance is changing. We're changing the charter on the NEIGB and that was done because of the data center consolidation effort we are doing, and we are robbing the clout of that body. Better governance is required as an enabling function in linking the warfighter and the business requirements of the budget. Everybody that I talk to believes that a network is a weapons system, any Sailor on any keyboard is a user of that weapons system and sometimes that creates a vulnerability that we have to account for. So it's important work.

We are doing a lot of work with information assurance. In the variation reduction category, and tying in with that data center consolidation, we are making known that resource sponsors are going to have to get their applications in order. Janice is working hard on the FAM process to help that along. We are also using our approval process on an automated tool for the info dominance approval system, which is showing some good work. We have to get visibility into what's called "grey IT funding." We've got about 9500 users and have had 25,000 requests so far and we've captured \$3.5 billion or so of non-continuity of service contract NGEN IT money. That's a success story and that's an area where we need to continue going down the path.

Couple of comments about JIE - Navy's on board with JIE. We are actually making really good progress. Depending on who you talk to, there are some cases of Navy being our usual defiant self, but I'll say we have a questioning attitude about the path we're on in pursuit of JIE, but we're not questioning the value of what JIE will bring in terms of the way we do our business.

We're making good progress on what was called "The Big Rocks." Application rationalization, data center consolidation, enterprise services, identity and access management, and single security architecture. Navy is doing things in all those areas and progressing the ball. But in all those cases, and specifically in JIE, it's important that we look at the value proposition and make sure that we are getting a competitive product at a good cost. We will continue to work it in the building with DoD CIO and the other services as we go forward.

That's probably enough as an opener, let me pass it to you.

Robin Thomas: Good morning. So, in reemphasizing the Marine Corps effort to contribute to the savings attributed to the DON, we are continuing to enforce our policy on use of enterprise licensing agreements. We are maturing our process of IT process management after going back to the government owned and operated environment. We're continuing to rationalize applications and systems and we are continuing to plan the migration of these applications into our data centers.

We are continuing our planning for virtualization. We are looking at the concept of mobility and how that can save the Marine Corps money. We've invested in some tools to build out our

enterprise architecture and use that as a decision support tool, as well as improve our portfolio managers' ability to manage their portfolios. As far as JIE we are actively engaged. We have dedicated resources to help develop those architectures, the standards, the TTPs. And we continue to work collaboratively with that team.

I think that's all that I have to say as opening remarks. Thank you.

Terry Halvorsen: Ok, over to you guys. What questions do you have?

Audience Member: If I may, there are some concerns that I've had. I'm stationed at China Lake so I thought I'd bring this up now. My question is why aren't there any hot backup sites for NAV-IDAS and for DADMS if we are really looking at information dominance and information superiority?

Terry Halvorsen: I think the first answer is because we haven't funded them. The second part is that we have a lot of things that we need to prioritize for hot backup. So I would argue that for some of the systems you mentioned, hot backup may be the desired, but it's not actually the requirement. To be able to restore that data quickly, and data back up and data restoration are two different topics. What we want is to be able to restore that data quickly. There is funding in both the Navy and Marine Corps and DON-wide to improve our ability to restore those systems quicker. The thing that we need to decide is how quick is quick.

The cost for data restoration goes along timelines. You want 24 hour restoration? That's one price. You want 72 hour restoration? That's a better price. So we need to make sure we understand the requirements. What are the impacts to both the weapons systems and the labs, in terms of timeline to restore that data? I think I would argue that from what I've seen, a 72 hour restoration would be a good balance point. But Navy and Marine Corps operationally are going to have to weigh in with that and come to their own conclusions. I don't think those systems go to hot backup. I don't think they generate that kind of cost requirement, but they definitely need a better restoration than what we have today.

Janice Haith: On the NAV-IDAS system we are working with NAVAIR who is basically the executive agent to get a more robust COOP capability and we will host it probably at Charleston. But we are working it, and Terry's right. We don't believe it requires that hot COOP that a lot of people do. We think it costs way too much to do that, but agree with the 72 hour restoration. We have money identified this year to make that happen.

Audience Member: I have a follow-up question to that. In DADMS, there is a questionnaire that requires a lot of detail. With all the applications that we have, in going through the FAMs we are finding that it takes a very long time to get a new application registered. These questionnaires seem to be very long and arduous. What if it was simplified to the point of asking what is it? Who we are? What network is it going to be on? And how long do you plan on using it? Or something like that. Is there any more value beyond that?

Janice Haith: Let me give you some insight to the FAMs and what we are doing. We are restructuring the FAMs and working to streamline the whole process so that we can get down to

about seven FAMs on the Navy side. It's a work in progress. Part of the problem that we are having is we have a lot of applications. If you look at our total portfolio we have over 26,000. We are trying to reduce that inventory but we also have a challenge that many of our applications are not at the state that they should be. And we have to get them to a better state in addition to rationalizing. So it's a process and it will happen over the next two to three years.

Terry Halvorsen: So I think we are probably asking for a little more detail than we should, but we have to do that for a while. The history of where we've been with the FAM process is not a happy history. We can't define the cost very well for a lot of applications, which is part of what we are trying to get to with some of the questions. Here's an interesting fact, within the DON, we actually did close a lot of applications. And you know it was amazing, all of those applications apparently were free. So we've got to get more data and change the way we are doing things. There is going to be some pain across the Department. We are doing the same thing at the Secretariat level, hearing the same kind of questions and concerns. But this process has got to get better. We've got to understand what we're going to cut, what the costs are, what the implications are, what are the security risks?

One of the topics I'm sure is going to come up today, call it XP eradication, call it Windows 7 rollout, they are the same process. We have been putting out that Win XP is going away. We are still not very well prepared in certain segments to get that done. Part of what we are tracking in DADMS is why we didn't at least know that hey if you can't get that and there's money, that should have been a concern that came forward, and a lot of application owners did not do that.

Adm. Branch: Application owners are like everybody else, it's not a priority for you until it's a priority for you. And it's not a priority for you until it's not going to be on the network. As we learned over the course of the fall, there are a lot of vulnerabilities out there, and as we increase the security posture of the network that would entail a lot of applications that will no longer plug in. It's funding issues for everyone. We won't cure it all at one time but we have to move in that direction, and it's not a clean process. I understand your frustration, and I know it's frustrating and a pain to do all that data entry. We are open to suggestions for streamlining the process and making the process better, but we have to go down that path.

Robin Thomas: I would just say that I haven't really heard that from Marine Corps system owners, but that information is needed for the FAMs to determine if that application or system is providing a service that is already being provided. That's what it's about, not adding to the portfolios, but reducing them.

Audience Member: I have a two part question. Now that the NOCs report directly to Cybercom, does N2N6 have the ability to task the NOC, and do you have the ability between the CIO and N2N6 to implement strategies through these types of tasks?

Adm. Branch: I'll start by saying that there is no line, dotted or otherwise, between N2N6 and Cybercom. And if I've got that wrong you guys can fix me, but I think that's correct. So there's task and there's ask. What do we need to do collaboratively in pursuit of better operations and IT strategy moving forward? There are some things when it comes to hardware that the governance

process would get involved in, but it's not a direct line with tasking authority to make that happen.

Terry Halvorsen: I don't actually think there are any issues with the development of the strategies right now. We are all certainly learning lessons about how the integration of that C2 is going to work, but I think that more at the tactical level and it's not impacting where we are going with our overall strategies.

We have an integrated strategy for the DON. It's part of our strategy to get to JIE, to get to common capabilities. That's happening. We are programming money to support the journey to get to those strategies. I don't think that the mock chain of command issues are impacting our ability to do our strategic planning at all, and I think we are aligned to the end state of JIE. The difference is sometimes we have a different pathway to get to that end state, but I don't think that's impacting strategies today.

Audience Member: Talking about streamlining, after all the applications are rationalized and reduced down to that magic number we are looking for, have we thought about incentivizing the publishers of these applications? We use more COTS to meet those requirements beforehand so that when we do get their licenses, to try to get them to start thinking about getting their applications to meet our standards. We do spend a lot of money with these guys and we are a pretty good share of their market.

Terry Halvorsen: The answer to that is absolutely yes. You could probably talk all day on that topic. We wrap that around the enterprise license agreements. Part of when we do enterprise license agreements, and we've done two of them, is to get providers to change some of the standards of what they provide and get our own requirements into the license agreement and sometimes even into products. We include a discussion about getting future products at the same time, so all of that is ongoing. I think we have been very aggressive with the two services. I think they have taken that dialogue and said hey we do spend a lot here, and the response from industry has been supportive. Oracle and Microsoft have been very forthcoming with here's the data, here's what you have been spending with us, here's what we think you could do to reduce spending with us. We've have a lot of success. That effort is up over \$60 million in savings and on track to exceed what we had predicted.

Audience Member: My question is dealing with the bigger picture. We're talking about IT here, but I want to talk about OT on the industrial controls system side of the house. What are we doing to ensure that we make that program a program of record so we don't have to keep nickel and diming other parts of the IT community to support the industrial controls system for the Department of the Navy?

Terry Halvorsen: We're not doing anything right now to make that a program of record. I would tell you we are looking more at the governance. But at the Department of Navy level that is not on track right now to become a program of record, we are looking at the way we govern that. One of the things we have to look at, we do an awful lot of testing, and we have an awful lot of money invested in an awful lot of test facilities. We've got to look at the business and technical process of how we do our testing. Is it the right way? Are we leveraging our tests right?

Are we in fact in some cases duplicating testing at various levels? So that's the first thing that's coming down from the Secretariat level. How we do look at the entire test model to see if the right process is in place. I think once we have the answer to that, that will give us a better picture of if it needs to be program of record or if it can sustain its self now or do we have to make some reductions in our current testing facilities, or maybe change what some of the facilities are doing. And if we can repurpose some of the facilities to do that it saves us a lot of money from having to recreate testing. We also have to figure out how, when we are buying commercial, leverage the testing that the commercial world has already done. We don't leverage well enough what the commercial world has already done. We are hesitant to do that from a trust standpoint. On the industry side, in the past, they have not been as willing as they are today to share all of their testing data.

Janice Haith: One of the things we need to make sure everyone understands is that the CNO and Mr. Stackly designated SPAWAR 5-0 to be the IT tech authority. So many of the things on the industrial side where we have not had oversight or standards to assure that we have interoperability, are in the process of happening. They are working that now but it is a process. It won't happen overnight, and we think in the next 2-3 years you will see a major change in that area.

Audience Member: Are you able to comment on the concept of security as a service? I.e. instead of the government purchasing network encrypters, a company could provide a business case where you could set up an arrangement to just buy the service and the company could provide software upgrades, and things like that.

Terry Halvorsen: We are open to any of those types of discussions and interested to see what kind of business case you could put forward. I think the first thing we would look at would be on NIPR because we are taking less risk there. But we are open to ideas, so if you've got a business case send it forward, share it with the services and see if that makes sense from both a mission and security and cost standpoint.

Audience Member: You mentioned earlier Windows 7 migration, Windows XP eradication, what are some of the lessons learned moving forward to Windows 8 and newer operating systems, one from turning over an enterprise, but equally important, turning over tactical assets and then being capable of turning over an afloat system?

Terry Halvorsen: The first lesson that we've got to learn is we've got to actually enforce the timelines to start doing the work. If we had driven more of those timelines earlier, we wouldn't have the issue of some of the tactical systems are going to take a little longer. We need to do some of that analysis. The second thing is we've got to pay attention to what's happening in the commercial sector. Unlike pure weapons systems, in the IT market a big part is driven by where the commercial market goes. The other we've got to do is a better job of collecting lessons learned across all of the systems. One of the things I've seen is when we went to Win 7 there were a lot of common problems across different systems. We did not collect those lessons learned like we should have. So we could have put out guidance for those systems what to do when they went to Win 7.

Audience Member: We have a lot of systems that migrated to Windows 7 from XP but for some reason there was a disconnect. Windows 7 Pro is listed in DADMS as an approved application and operating system, yet it is not approved. So there are a lot of systems that have purchased Windows 7 Pro that are now facing the problem of trying to upgrade. I wonder if there is a solution like checking for a Windows 8 operating system. There is no evidence that that is in process of being evaluated or approved as an operating system. I wonder how that can be resolved at a higher level because a lot of programs have, just because Windows 7 Pro was in DADMS, have purchased that, and it's not a secure or approved operating system.

Terry Halvorsen: I think we want to get more detail on your questions and work that offline. A couple of things, if you bought Windows 7 Pro there may be some reasons for that, but that is not one of the approved sets of licensing so we need to find out where that broke down, so we ask that you talk with Janice and we'll get you a better answer on that.

Audience Member: I have a question about what is the Department doing both in policy and mandates as well as budgeting and spending money to comply with the defense authorization language that's now in there about software assurance. For example, the Air Force in the past has stood up a software assurance center of excellence. If it's just a hey all you programs you've got to do this, that's fine, but we'd just like to hear what the Department is doing.

Terry Halvorsen: The Department has had direction out on that since '10 that says we will buy, use, and ensure that our contracts include software assurance. Both the Navy and the Marine Corps have that signed policy.

Audience Member: Good morning, a question regarding on Tuesday, Deputy Secretary Fox mentioned that one of the main concerns is actually retention of the civilian workforce. I think as we are being pressed right now into new dynamics with the network now being considered a weapon and as we are facing increasing cyber threats, what are some thoughts on how we can retain our cybersecurity and cyberspace workforce as well as attract new personnel with those same skill sets?

Terry Halvorsen: We are going to have a big challenge with that. I think if we try to pretend that we're not that's wrong. We are going to have a huge problem retaining civilian and military. We are already seeing issues with those who have IA certifications. We are working on a manpower strategy. There is a panel looking at what is doable. The simple answer would be to say we pay more. I don't think that globally that's going to happen. We have to look at what are the opportunities we can offer coming into the Department of Defense. It's always been true you will certainly get a more global view and more opportunities to make a wider impact. We've got to stress that. How do you have a cyber/workforce development path for civilians? That is not something routinely seen. I think in this area because of the pressure we are going to face from industry in keeping that workforce we're going to have to have a more structured career development path and offer some more growth opportunities for the civilian cyber workforce. I would let Twig and everybody else comment on the military.

Adm. Branch: On the civilian side clearly we didn't do ourselves any favors over the last few months or over the last few years. Three years without a pay raise and furloughs last year. With

the government budgeting debacle that we went through just didn't instill confidence in anybody that the people in charge are making the right decisions. We don't even realize the cost of that in decisions that people are going to make with moving out of the government.

I think it's also obvious in this environment with the advances in IT and particularly in the increased visibility and the requirements for IA and being savvy about network security, there will be a big job market available to all of our workforces, and many will head that call and launch off to industry.

Some of it is about leadership and telling people they are appreciated. Some of it is about quality service and of work/life balance and trying to accommodate our schedules. Part of it is about doing things that you can't do anywhere else. Particularly in the cyber world we have a lot of people, Sailors primarily, that do that work for us because they can do some neat things that they can't do anywhere else. That is certainly an attraction and it's been an attraction in the military for a long time. We will try to incentivize where we have shortages and that's a pretty data free statement to say that. That's what we do. We wait until it's too late then try to recover from the divot we have as people leave. That's just reality and I think you can expect that. We need to try to get ahead of that curve and be good at predicting where the shortages are going to be and work to fill those holes. As we go down this path and decide the workforce we need we are probably going to have to think about, well is it important that this guy can run a mile or do pull-ups, or is it important that they know what they are doing around the network. In terms of recruiting for the workforce of the future, we need to think about maybe going after some non-standard careerists.

Robin Thomas: Speaking for the civilian community and really more intangible things, we do have a robust ITM community of interest, that's led by our deputy, Mr. Jack. We've got a pretty robust portal that reaches out to that community. Also we are encouraging folks when they do have openings to advertise those as career ladder positions so folks can come in on a lower grade and stay around a couple of years. On an annual basis have actually had a budget for training for that COI. This coming year we will be expanding our C4 awards to those folks who are executing some of those CIO core competencies.

Audience Member: Good morning, I wasn't going to stand up and ask a question, but you opened the door Admiral. Being a 30 year retired master chief now working as a 2210 and loving it, but I was out of work for 20 days before I went back to work. You brought up the subject of furloughs, and what I ran into was that when all the civilians left there was no military in place to be able to do some of the IT troubleshooting and other things. I was wondering if we've thought about what to do if it happens again so that we don't have Sailors going weeks without access to NMCI, or without a productive way of doing their job.

Terry Halvorsen: The answer is yes we have thought about that. I don't know any organization that's going to take over half of its organization, send it home, and then say what do we do when that happens. Certainly there are some lessons learned. We have opened the avenue to what people can be protected from. A better answer is that the Department of Navy has no plans this year to furlough in response to any of the budget issues. We are not planning any major reduction in force. I think that our leadership particularly during all of this, was very vocal about this was not a smart plan. It happened, we are still learning lessons, but I will tell you the guidance was that it's not an option for us this year to deal with our budget issues.

Audience Member: Thank you for that, I'll take that back to my command. That's something reassuring for all of us in the civilian workforce to know.

Adm. Branch: I'll just reiterate that there is no appetite in the Navy to go there again. We recognize the value of the service and it's just not any good way to do business. People understand the damage that causes and we are still analyzing that. CNO has said it; I've heard SECNAV say it, we're not going there again. Now, do they have the final word, no. But throughout DoD there is recognition that it was a bad idea.

To your point of Sailors having to do the job that civilians had done, that didn't happen by accident. We got to the point where we are with the civilian share of the workforce for good reasons. One of the reasons was to draw manpower down and part of the business case was that it could be done at a better value by a civilian as opposed to a uniform. We could always go back and look at those cases, but I think that's where we are and there won't be any major effort to try to bring in a whole core of relievers. We have Sailors going where Sailors need to be and civilians where they need to be and can be, and I don't see any restructuring going on.

Terry Halvorsen: There are no plans to restructure that workforce.

Audience Member: Good morning. I would ask the panel to consider allowing local commanding officers the authority to issue, the authority to operate those systems that do not connect to the DoD IN, or to the DoD GIG. Those that are local, or those which are closed.

Terry Halvorsen: I'm going to take this. No. I'm sorry, we got into a really bad state and we can't go into all the details or where we are today but I don't see us issuing that policy. We have given that authority to Twig and Kevin and I think they are doing an excellent job, and there are no plans to change that policy.

Audience Member: Are there other initiatives available to reduce the rework, reduce the churn, and get the packages through faster? That's what my goal was, to improve this process.

Terry Halvorsen: If your goal was to improve the process, I think we all understand. So having some familiarity with this over the last 8 years, we've gone up and down. In '05, it was 396 days to get a package through. That came down to under 120, we are now back up to about 190. We are certainly all engaged with how to improve that.

We are looking at two levels of change. One I will call the tactical level and see if there are some better tools we can use to reduce the paperwork. The other is the operational level, and what DoD and the rest of the government is doing, how do we incorporate that into the system. Not only do we have all of the resource sponsors at Navy involved, but we've got the operational parts involved in that. I think you'll see some immediate changes probably at the tactical level that will save us 10 or 12 days coming out by the end of March. The bigger piece will take a little longer because the other thing we have to do is make sure that after we've made that change that we understand the process well enough that we didn't just introduce a vulnerability to the process.

So I would fully admit that right now we are a little bit over-conservative with that process, but for some good reasons. We understand that, but we are really going to take the time and walk the process backward and make sure we don't lose anything as we change and streamline it.

Ok, thank you. We do take the feedback seriously. If you didn't get a question out that you wanted answer, you all know my email. You will get an answer, it may not be the next day, but you will get a response. So thank you for your time and thank you for your questions.