Remarks and Q&A by Dawn Meyerriecks
Deputy Director of Acquisition and Technology
Office of the Director of National Intelligence

***Defense Daily's* Cyber Security Summit**
Washington, D.C.

June 11, 2010

GEOFF FEIN, Co-CHAIR: I want to introduce our keynote speaker this morning. Dawn Meyerriecks became the deputy director of national intelligence for acquisition and technology in September 2009. Before her current employment, Ms. Meyerriecks had worked as an independent consultant for government and commercial clients.

Previously, she was a senior vice president for AOL product technologies, where she was responsible for the full life-cycle development and integration of all consumer-facing AOL products and services, including the relaunch of aol.com, AOL Instant Messenger and the open client platform. Ladies and gentlemen, please welcome Ms. Dawn Meyerriecks.

(Applause.)

DAWN MEYERRIECKS: Good morning.

(Chorus of, "Good morning.")

MS. MEYERRIECKS: Aw, that's not bad for 8:30. I'm pretty impressed here. I want to thank *Defense Daily* for allowing us to be here this morning. And I have only a handful of slides which is kind of my trademark. I am definitely opinionated. I still hear music in the background but maybe that's what you prefer; I don't know. I'm not used to speaking to violins, but – (laughter); normally not the reception that I get.

But hopefully, we'll have time for some dialogue. And I like interactions because that way I know the coffee has kicked in and we're actually all on the same sheet here. So without any further ado, let me see if I can get to my slides.

(Off-side conversation.)

All right, so why don't I just get started. And if the slides show up, they'll show up; and if they don't, I'm perfectly comfortable with that, too.

So what I wanted to talk to you about today is a federal cyber security initiative that is planned to be put in place in the FY '13 timeframe in which we are collaborating and very much interested in, in the initiatives as they move forward.

We are involved in the – with the office of the OSTP, the Office of Science and Technology for the President, with – looks like someone's going to come help me here – with defining three major initiatives that we believe underpin the future of how we ought to think about cyber security in the country.

And let me just table something here that I have in my slides but I think is really important: Cyber security is not the same as information assurance. And we as a community talk about those like they're interchangeable. And one of the things I'd like to leave you with, if you take nothing else away from this, is that we need to clean up our act as a community. They are not the same things. We should not talk about them as though they are interchangeable.

Information assurance is about risk management as it pertains to IT assets in general and it includes the soft as well as the hard components of that. Cyber security is very much focused on computer security and it's not necessarily about risk management. And I think when we mix those two things, we do a disservice to our community but also to our leadership because then they equate those two things, and they are not the same thing. So let me just put that out there.

Now that my slides are up, I'll actually continue with where we were going to go. Let me give you a feel for the mission as we view it from the DNI but, more broadly, from threats to our health and welfare as a society.

One of the things that we think about is if you can address the Straits of Taiwan through radical militant groups that may or may not have state associations, then that's pretty much the spectrum that we deal with. We deal with – we'll call them lone wolves; the 12/25 bomber, and the whole way to nation states that might be interested in undermining our stability or otherwise upsetting our way of life. And that's the spectrum that we deal with.

The interesting thing is that technology is completely agnostic in terms of how it gets employed or where it gets employed. And I just have a couple of examples up here. There are plenty of these. You can, for example, build a machine – design a machine – highly complex plastic parts, high impact, high-ingest plastics with a $300 machine that you can have in your home.

Do-it-yourself drones is a very, very capable website in terms of if you want to build something fairly significant and drop stuff from it. LavaAmp is a $100 gene sequencer that is commercially – or, will shortly be commercially available. Locomotors.com is really interesting and I put the websites there.

Based on your interest, you can go figure these out or look at them. You can actually design a custom racecar over a weekend, build it and drive it home. It's a place in Texas. And what they do is they use a bunch of component parts, allow you to assemble them pretty much any way that you'd like and drive it home.

And what they figured out is that the crash rules only apply if more than 50 percent of your vehicle is aimed at a commercial market and it's not customized. So I'm not sure you can get these insured or how you would insure them, but the fact of the matter is, is that technology has been democratized to the extent that it's not just cyber; it's the physical world as well. So it's the virtual and the physical.

And then of course, World of Warcraft, Facebook; there are all sorts of things that go on that allow us to collaborate in ways that it's not just us, right; our enemies know how to do this. People who want to undermine us can use hard and soft technologies in order to figure out how they can come at us.

And so the trick for us is we have to be able to stay ahead in terms of how we aggregate these things and think differently about the problem. And that's really what the federal cyber security research agenda is about.

So one of the things people say to me, well, don't you go home and lose sleep at night in your job? No, actually, I don't. And part of the reason is not because this technology isn't available to everyone. It's because our social structure scales in a much better and more purposeful way than our adversaries do at this point. And that's our advantage today.

We can't count on that forever but, for example, nobody has the combination of the military, DHS and the other things that are going on that are able to get together. And you can read all about how much trouble we have with that but I would submit that we're still better at it by far than any of our adversaries. So we have a scale and a breadth from a social perspective, from a soft perspective, that allows us to apply the technologies in ways that allow us to be competitive and actually stay ahead. And that's the thing that keeps us going.

But from a technology perspective, what should we be thinking about from a cyber security? And let me tell you, we'll get to that, but here's just an example and this is DOD example and it's dated, but Desert Storm versus Iraqi Freedom – it's dated but it tells you what the force multiplier is if you can combine the social with the technological.

And the one that I point out all the time is if you look at the number of platforms per target versus targets per platform, for Desert Storm, it took four platforms to get a single target. In Operation Iraqi Freedom, which was roughly a decade later, one aircraft could take out four targets.

So those are the sorts of force multipliers if you can combine – and it's not just technology. You also have to combine the ability to scale from a social perspective. The fact that the services got together, intel got better-integrated – that's what ended up making the difference between those two decade-apart activities. It wasn't just that technology got better. It's actually we figured out from a social perspective how to graph those things together so that we were much, much more effective.

So here's my rant that I talked about when we started about cyber security versus information assurance. Again, if we can talk about this clearly because the people in this room understand these differences, then we won't be confuting the two. Information assurance is all about risk management.

So I'm going to say something that I hope is not a surprise here: There will never be a perfectly secure computer that's connected to a network. I'm just going to assert that. So we've got to think about the problems.

We are interested in information assurance. At the same time, we are looking at the discipline of cyber security because that's how we're going to try and raise the bar in terms of how we're protecting. And in fact, in some cases, that's a trade space.

When I get in my car and I'm driving around – and I live way out in the boonies – the things that I watch for are things like deer and raccoons and things like that. When I'm in D.C., I'm not watching for deer and raccoons. I'm watching for the cab driver who's going to come into my lane or the bus driver who's going to use the (load ?) gross tonnage because he just can and be in my space.

And that's the way we've got to think about this problem. Information assurance is about risk management. Cyber security is about how we handle one aspect – the discipline associated with one aspect of how we deal with information assurance. And I think that's really important that we not confute those two things.

So given that, so hopefully everybody gets that this cyber security research agenda is not about information assurance; it's about cyber security because that's really important because this is a continuum that we're going to have to balance.

So here are the three initiatives. I think this is interesting because it's going to generally be administered outside of the DOD and, clearly, outside of the intelligence community, but very important to us because we do lots and lots of business in that space.

Tailor trustworthy spaces – and I have a slide on each one of these; moving target and cyber economics, with the idea that there will be multiple billions of dollars put into these initiatives in the FY ’13 time, and maybe some in FY ’12 depending on how we work things out with Congress in terms of how the funding flows. So let me talk to each one of these and, hopefully, these will spur some questions or some conversation during the Q&A.

Tailor trustworthy spaces: I talked a little bit about when I’m driving in Purcellville versus when I’m driving in D.C., I think differently about the problem. When you go to the library – if you go to the library – so maybe that’s not a good one to start with, but we’ll start there.

Let’s talk about a theater. When you go to a theater, there are certain rules of behavior. And there are certain expectations that you have and transaction in terms of the ticket. You expect that people are going to be quiet around you because they’re there to see the movie, too. When you go to a ball game, totally different experience.

And so one of the mistakes that we think we’ve made is we’re trying to float the whole level of the ocean higher. And we’re much more sophisticated than that. Our expectations of our fellow people and how they will act in different situations is tailored to the environment. And in fact, the morays of behavior are different based on where you are.

At a ball game, if you sit there and behave like you’re in a theater, the people around you are probably going to wonder, like, why did you come, right? If you kind of just sit there and you’re very quiet and you don’t jump up and down and scream when your team scores a run or whatever. It’s kind of like, wow, that was weird; why did they bother coming?

If you do that in a movie, you’ll probably be escorted out. And so we’ve been way too unsophisticated, way too naïve. We’ve tried to make things – we’re a bunch of technologists. We try to make things zeros and ones. The world is not that simple. Cyber security is not going to be that simple either. So that’s the idea, is that we have to be much more sophisticated in terms of the runtime environment that we expect based on what kinds of transactions we expect to be carrying on.

So for example, if I’m doing an interchange with my bank, I want that to work 100 percent of the time, every time. There are other examples where I refresh a page in Google when I Google something because it’s taking too long. I get nervous if I have to refresh the page with my bank all the time. But if I’m just doing a search for who won the ball game last night, if CNN is slow and I can get it from ESPN, okay, I’ll just cancel out of that and keep going. And that’s okay. We’re all sophisticated enough to figure that out.

And one of the precepts that we think we've messed up is we tried to do a 0/1 kind of approach to this and somehow we're going to make – from AOL, we always talked about "my mom," right? Not "my" mom but the generic "my mom." I'm never going to make my mom's computer not subject to being part of a botnet because my mom – I love my mom – she's just not very sophisticated in terms of IT. She calls me when the printer runs out of paper – no, seriously; it's like, that's how – come on, we all have moms, right, or dads or somebody – Auntie Mae that calls you and says, my computer's broken – or somebody – maybe it's you but we won't raise hands here.

But that's the point. My mom's computer is probably always going to be part of a botnet no matter how many times I clean it up because she's going to hit yes because she's going to get to her bridge game or whatever it is she's going to do.

And we're all trained. How many of you totally read the T's and C's whenever you get an upgrade from Apple or PC – anybody? Okay, so we're all vulnerable because we've all been trained – and my mom's no different – to say when it pops up, it says should I continue? Well, yeah.

And in fact – and I tell this story and it's really sad but the DOD and the IC don't actually load the certificates in for external sites. So we've actually trained our own people to say, I don't trust the certificate; should I continue? And we say yes, of course. That's the way it works because we don't have those in there.

So lots of examples of this. That's just life. But that's okay because my mom is never also going to do banking on her computer. So maybe it's not okay because she's going to be part of some Russian gang that's going to be stealing money, but in terms of what's at risk there, she doesn't do her banking on her computer.

Now, in my case, it makes me a little more nervous that we've trained everybody in the IC and the DOD to say, oh, yes, I understand that I don't trust the certificate but I'm going to keep going. And we only do that on certain sites.

When I was a consultant, I had to do that in order to get paid; had to say yes, I trust the certificate of a DOD site that I actually logged into in order to get paid. That's okay; I had the context to make those sorts of decisions. And that's the environment that we need to create.

This relates to the last initiative. And I'll just tell this story quickly. At AOL, we found that customers would trade convenience for security every time; every time. If something got in the way of convenience, they would immediately abandon any need for security. Were they that overt about it? Yeah, pretty much. We had people that – their accounts had been phished, we would upgrade them to a fob and in six months, they were not using it.

Now, they had suffered, in many cases, financial loss overtly because they had been phished. And in six months, it wasn't worth the time and attention to take the fob – probably because they lost it, honestly – to enter that extra number in to make sure that their identity wasn't phished. I mean, that's just people. We can all rant about it but my mom's never going to be a computer science expert and she's never going to make sure that her computer is clean.

So what we've got to do is create the kinds of environments where there are different levels of trust, that there's an easy way for us to figure that out, kind of, in situations and make it painless so that somebody can actually, with some sense, say, yes, I'm okay that I actually don't know about this certificate, but I'm going to continue. And we've got to make that possible for people potentially like my mom, as well as for more sophisticated users like I like to think I am.

But I don't read the T's and C's either so, I mean, T's and C's are not a good way to get us something like this. So there's a whole lot of work that needs to be done here. You see the challenges associated with this. We might not even be thinking about the problem correctly and that's part of what this is about. It's to think differently about the problem but know that a simple model, a zero or one, is not a good model.

Moving target: So this is the – if you're on thin ice, speed is your ally, right? Go fast. So one of the things we're talking about here is, maybe standardizing to the same release of Adobe for 25 months because that's how long it takes us to validate the next release isn't a good approach. Maybe we ought to think differently about the problem. Maybe we ought to move quickly and then have a staggered baseline so that we're not vulnerable across the board.

In fact, another example – another AOL example because they're unclassified and dated at this point, so I'm okay with those – the load-balancing piece of software that actually shoved, you know, 30,000 IM users that all wanted to log in at the same time in the morning to a particular server set got overwritten constantly.

And I mean, by us, so that we could preserve the CM baseline because we knew that was one place of vulnerability that could be – if it were exploited, could actually bring the service down. And, you know, service outage is a really bad thing. So there's different – so we constantly overwrote that to make sure that it wasn't getting changed. Because you know, if we did it often enough, we could control it.

So there are very different approaches to how you do this. And I would submit that AOL is not the only one who is doing things like this, but it's a fundamentally different way of thinking about the problem. And there, again, you know, there's some basic things like run time, configuration management, that classically, the government's not so great out, that has to be in place in order to make this work.

So there are some significant challenges here, but a different way of thinking about the problem is to move and move very quickly. We're not saying in this particular one that we think this is the answer, but we think we ought to have the conversation and understand whether or not there are some benefits here.

And based on my previous chart, which was different risks, different environments, maybe there's a class of problems that this is exactly the answer that we should be thinking about, as opposed to a very stable CM baseline that is, you know, tightly controlled and kind of just chugs along at a validation rate.

And then the last one, the cyber economic incentives – so here, this kind of wraps back into the things I've been talking about. What will motivate, or cause my mom – if I ask my mom if she wanted her computer to be a botnet and part of a botnet, she would say no. So what would motivate her? What's the threshold level of pain? How trivial would it have to be for her to be able to validate – you know, what would she be willing to do to make sure that her computer wasn't part of a botnet?

That probably is different than what I would be willing to do on my classified system that I use for the intelligence community, right? There's a different expectation level there. And how do you motivate that? Now, in my case, you know, if my computer gets compromised because I did something like put a thumb drive in or said yes to – yeah, go ahead and download that, you know, key-click follower – that would be different.

There are repercussions for me. But in general, if we're trying – if part of our effort is to raise the level of the ocean so there are fewer TAC platforms out there in the wild, then the impedance factor for my mom to be able to be part of that solution has to be much lower than it is today, right? So how do we get at that? And how do we motivate?

And I think, also, I'll throw something out here. You know, people talk about, well, we ought to make the vendors ensure their software. Okay, so how much has insurance stopped the spread of cancer? Is that the right model? And obviously because I asked the question that way, I have an opinion on that – (chuckles) – because I could have used lots of other examples.

But it depends on how you think about the problem that we're trying to address and how it ought to be countered that makes a difference in this space. And what we're saying is, if we agree we want to raise the level of the wild so there are fewer things out there to worry about, how do you do that? I used my story about AOL and people that had been fished. And it's just, you know, consumers will trade ease of use for security every time, even when they personally have suffered financial lose. So how do you address this?

So those are the three initiatives that we're talking about. They're very broad. We don't have any fixed ideas about what the answers are. I just think they're very, very good questions because they try to get at the – cyber has to more closely resemble the trade space that we make in our own lives.

And it has to be presented in a way that it feels intuitive to us, so that we can – you know, okay, this bus is going to pull into my lane, so I know I need to move. Those sorts of – I don't even think about that anymore. I just anticipate that it's going to happen. So those sorts of things.

Now, it also says there are risks that we all incur that we don't think about. And that balance needs to made, right? I get on an airplane. I got back from Seattle last night. I didn't think anything about boarding the airplane. I wasn't worried about whether I was going to die on the airplane. But we don't have those rules in place. We don't know how you even think about that from a cyber perspective, right? We don't have a risk context that makes sense to us.

So there's a lot of work here. This is why it's being sponsored at the federal level. This is not a – there's not an answer band-aid that is going to come with this. A lot of good, thoughtful work needs to happen. So I think here are the opportunities. Help us by talking about cyber security versus information assurance. And I'd love to have a discussion if you think those two things are interchangeable. And again, you know, I think we do a disservice when we talk about them.

Let me table something, but this opportunity that – this funding that we're talking about is not a selling opportunity per se. We're trying to get at the intellectual struts for how we think about cyber and how we move forward in that space. And yes, products will probably come, but we're of the opinion that we don't have the intellectual fabric yet to actually be thoughtful about products.

We've got tons of products. Things have gotten better. I don't want to say anything – I don't want to take away from that. But we're starting to question whether or not the fundamental precepts are right and that's really what, at least initially, this will be aimed at. We're looking for traditional and nontraditional partnering in sourcing. You know, there are some good lessons from industry that we need to bring forward.

And you have to factor in – and I hope, hopefully have tabled some of this – the soft as well as the hard sciences. This isn't simply a computer-science drill. This is a, how do we actually get users to behave in a way that is helpful to us?

And I would encourage you, for this major initiative, there's a forum here. We are looking for ideas. It is open. We're actively soliciting those, or you can send an e-mail, but I encourage you – if you're interested in the space where the government's about to spend multiple billions of dollars to think through the intellectual struts, here – to register for the forum and get into that and provide feedback because we are actually looking that and trying to incorporate that in the first set of initiatives that are being formed right now to try and go after these three themes.

So here's my pitch. You're technologists, in general, here, or you wouldn't be here today. Demonstrably focus on mission outcomes. We've got to be about – what effect are we trying to achieve and how's the best way to get there? We're trying to raise the level of the water across, you know, the open Internet. Then how will we go after that? Or, you know, are we trying to protect highly classified intelligence assets? Two different problems, very different solution spaces, probably.

We need to collaborate. We need to be thinking about not just the classic Beltway answers, or not just the classic commercial answers – you know, this – well, commercial lessons learned apply to the DOD or the ICE. I hate that question because I think it's a bad question. The answer is obviously yes, but anything to an extreme is a bad answer.

I think we need to be really innovative because I think we're going to run out of runway on our current approach. I think everything, right now, looks like a nail, so we're using a lot of hammers and we don't need to be. And at the end of the day, this community is responsible to deliver innovative technology-based capabilities that solve intelligence challenges – not just my challenges, but of course that's my worldview. Those are the things I worry about – but in general the challenges associated with applying IT at the social level that we're talking about to be effective from a cyber security perspective for the nation's sake, not just the intelligence community's sake.

So, with that, I'm going to – that's my last slide. Everybody was – I did get a little bit of feedback because people laughed. So I know you stayed with me. Comments, questions? Sir.

QUESTION: First of all, when you made the comment that information assurance and cyber security are not the same thing, I was ready to cheer. (Laughter.) But then when you – you kind of – at least my impression of what you said, you kind of said cyber security is actually kind of smaller than IA and doesn't include risk management.

And I've got to tell you, my interaction with particularly the DOD folks is exactly the opposite. They are looking at cyber security as a bigger set, that IA is sort of a subset of it and it's totally about risk management. It's totally about – the first one, this one, the mission outcomes. Is your way of defining those, too, is that your opinion or is that NSA's? Because that's different than what I've heard before. I just – I'm not trying to get into an argument with you about it but that piece of it struck me as different from what I've been hearing.

MS. MEYERRIECKS: Let's see. So I think there is plenty of discussion here. And I won't say that mine is right and somebody else's is wrong. Again, this is part of what the problem is, I think, right? We don't have enough specificity and we don't have enough consensus in the community as to what set of problems we're trying to solve for what particular outcomes.

So, in my mind, it feels like a subset. But that's Dawn's worldview, right? And would I arm-wrestle you on that strenuously? No, but I'd love to have a conversation about that because I think part of what we've got to get at is what set of problems we're trying to solve. And the thing I think that gripes me most is when people use those interchangeably – information assurance and cyber security.

So I think we can have lots of robust dialogue about which is the elephant and which is the tail. And I'm not sure if, at the end of the day, if it matters a lot at this point. So, yes, I've heard – I'm friends with lots of people in the DOD that espouse that opinion. I have a different one. I think that's okay, not to die for. Sir?

QUESTION: Good morning, Dawn. On one of your earlier slides you talked a little bit about policy but then you didn't elaborate on it. It was back on your – (inaudible, off mike) – trustworthy; you mentioned – (inaudible) – policy, communication and policy specs and management as one of your bullets. Can you talk a little bit about what you had in mind there?

MS. MEYERRIECKS: Yes. Well, and, again, I'm going to use language that we understand today with the caveat that we may not be even talking about the problem right at this point. But that particular one is how – particularly for us – how we deal with multilevel classifications and things like that, right? There is a whole – if you know the intelligence community at all, there is a whole set of special things that we've been trying to work out pretty much since DNI was stood up in terms of this mismatch between categories and trying to share information across that.

That for us is the coherent policy implementation. But we had the same problem. If you expand that to DHS and what they're trying to do from a dot-gov perspective, right, there are different rules. For example, what the FBI is allowed to do with U.S. persons information is much different from what NSA is allowed to do with U.S. persons information.

That's the law, no choice about that, right? But how do you reconcile those two things? And then there is some technology that falls out of that. And my favorite example – and we were talking about one of the things in the car today coming over – we can, for example, I can be in a position where I'm allowed to see certain things.

But because I'm not wearing the right badge I actually have to go do special pushups in order to get access to that information. And it's that sort of, is there a way – and, again, if we're talking about the problem correctly today, which one could argue that we're not, shouldn't there be a way that says, okay, if Dawn, based on her position, gets access to all of these – and I'll pick on CIA special access categories – why do I have to go do pushups with CIA to get that added? When I joined the organization, why didn't that just happen?

And the problem is, we've got so many data sets with so many policy and access control lists on them that we've got it – the ways those get reconciled is you do one-offs. And that's what the tool is – you know, now we're starting to get to a tool and how do you figure that out. So is there - Are we even talking about the problem right?

And then there is the: How do we automate that so that it's not – for example, I showed up and six months later I finally have access to our shared drive at DNI. Bad on us, but I hadn't accessed it; I didn't know it existed. And then I found out I couldn't get to it. And it's our organizational shared drive so – it's that sort of stuff.

So there is a mechanical piece and then there is a philosophical piece about how do you work through that, both pieces.

QUESTION: I recently came from Wall Street back in to be a CIO for the government. And it's very interesting to me because, one, I work in a very unique environment because we are – (inaudible); we do RDT&E out on the island. But we're on NASA property. So all of my systems have to go through a point at NASA. So we own the buildings and test all sorts of – (inaudible) – things for all of the R&D – (inaudible) – the U.S.

So NASA does touch my network. So I'm looking at this as, I don't quite understand because I'm the new kid on the block, but I will tell you, I look at this and I go, what happened to best practices? We're always trying to reinvent the wheel here. You know, I look at what we do in investment banking and, you know, when is the last time somebody hacked into Goldman Sachs?

So why can't we hold ourselves to the same standards of global policy and push it down into a better – (inaudible) – you know, from your level push it down and say, okay, yes, you're NSA: here is what you should do; here is what you can look at and there just is no federation of people – (inaudible).

Everybody has their own policy. Everybody is throwing spaghetti at the wall, basically, and I am looking at the C&A package for IA going, risk management? I have 728 packages that I'm trying to get through and they are costing me about $250,000 for the one that's going through today. What kind of risk management is that? (Laughter.)

So I understand your point as far as IA being a risk-management tool, but we're not managing how we apply things; we're so busy trying to – anyways, sorry. I did have a question but now I went on a tangent and my rant. (Laughter.)

So I guess, looking from an outsider coming back in, my hope is that you guys will understand that we do need a federated architecture. And I've looked at the – (inaudible) - and all of this stuff. And you know, push it down as fast as you can because we're wasting money. That's my taxpaying dollar! So anyway, my two cents for it and thank you, it was very good to hear. I hope that once it gets pushed out to the lower levels, that it doesn't get skewed as much as it does in the upper –

MS. MEYERRIECKS: So I'll – let me respond to that in, just, two quick ways. One is that, again, one size doesn't fit all. So there are certainly – the risk – and you know, the risks that Goldman Sachs is willing to take, vis-à-vis AOL is very different.
So that commercial practice is, again, a spectrum, and we need to be sophisticated in how we think about that. Because what we do for, you know, NIPRNet may not be equivalent – may look more like AOL and Goldman Sachs, but what we do for my networks might look a lot more like Goldman Sachs, right?

QUESTION: Yeah – (inaudible, background noise) – form and function, right?

MS. MEYERRIECKS: Right. And the second is, what I always tell people is, don't do stupid, right? And so to the extent that – I don't know how to codify that as a policy from a DNI perspective. It's just that, you know, policy will never compensate, ever, for stupidity – (chuckles) – and you can quote me on that. So a one-size policy is never going to compensate for, you know, a runtime architecture that makes no sense – that's not reconcilable.

So that's where people like you, as the CIO, need to say, wait a minute. I have enough local authority – because I don't believe policy ever makes you do stupid, right? You have enough local authority to take your fate into your own hands and go work through that. And if you don't, then I would escalate it and decide whether or not it's going to be an issue for your boss to take on. Because if it's an accreditation authority thing, at the end of the day, the facility or the site owner is the accreditation authority and everybody else is an advisor, right.

So you can take a lot of this on at a very local level. You're in a very interesting situation, I understand – NASA versus all the various others. Yeah. But even within that, I would submit you could clean it up within the big stovepipes that exist. And so don't look for us, from the top, to figure this out because it's going to still be a local answer, right? What we're trying to do is create the framework so that we can have discussion between NASA and DOD at a leadership level that at least are apples and apples. And we don't have that right now. That's what this initiative is about.

(Applause.)

CAL BIESECKER, Co-CHAIR: Dawn, thank you.

(END)

As delivered, revised for clarity.