SPEAKERS:

THE HONORABLE DALE MEYERROSE, ASSOCIATE DIRECTOR OF NATIONAL INTELLIGENCE, AND CHIEF INFORMATION OFFICER

THE HONORABLE JOHN GRIMES CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

AUGUST 21, 2006

(Applause.)

DALE MEYERROSE: Thanks, Rich.

Boy, I was really impressed; you know, some ugly guy gets up here, you know, shaved head and moustache, goatee and says, shut up, and everybody sits down and shuts up. I've been in churches that weren't as quiet as this, and so I was really impressed.

Welcome. It is indeed an honor – thanks for honoring us with your presence, and it is our intent to make your time here worthwhile – worthwhile in a big way.

As Rich outlined a little bit, this is not your father or mother or brother or sister's Intelink conference. For several years many of you have being going to the Intelink conferences, and those have been successful in their own right, but they were missing something. They were opportunities for a lot of technical folks to get together to talk about issues, how to resolve them, but the thing that we were missing was the operational piece, the mission piece and the policy piece, because when we talk about things we need to change, the first thing we all talk about is the culture. So we decided that we would work very hard to get some really key players in here to address this every morning so that we have that context, so that when we look to work many of these issues and problems, we understand the why because the whys always control the hows. And so many of us are responsible for making sure we do

things right; we just need to make sure that we're doing the right things. And this is truly a changed environment.

Now, some of you may have noticed that my staff hoodwinked me into letting an acronym get created called DISCO. And they gave me this long pitch, didn't let me know what they were really after: You know, the DNI's Information Sharing Conference, are you okay with that, boss? You okay with that, boss? And then they said, okay, then you just approved DISCO. And that was – I guess it was okay. I think it's an excuse to bring out some old clothes that some of my folks had in the closet because they just yearn for the '70s.

But there is an analogy here. Think about it. In our business, the transformation that started in the '70s with ARPANET, and the business that not every person that used ARPANET had to know all the intricacies and vagaries of mosaic. All that started in the '70s. And the '70s laid the bedrock business for telecommunications and the marrying of telecommunications and data automations and all those kinds of things, and I think by and large, if you look back in the lexicon you find, you know, information starting to creep into the lexicon, and so there is a circle which ties all those things together.

You know, you could say that a little bit of history ties what we're doing today. You know, today is the day in 1944 that Paris was freed. So some of you can maybe thing that you came to Colorado to get free from wherever you happened to be, like Washington, D.C. Or this is also the anniversary of 1858, the first of the Lincoln-Douglas debates in Illinois. Some of you may or may not remember 1858; Abe Lincoln lost in the senatorial elections in Illinois. But the debates started then, and they were famous for the issues that they sought to galvanize, so hopefully the debate that we have here today will hopefully galvanize. Today is also the anniversary of 1959 when President Eisenhower inked the bill which authorized the creation of the 50th state in the United States, Hawaii. And so maybe we can think about the business of some of the things, the relationships, the things we do here will actually establish things of permanence that we can go back, take with us, and work through the challenges that lie ahead of us.

That's as good as I can do to stretch all the history things in the making today relevant. And it took a long time to do that, believe me. What I'd like to do now is to transition into our first segment, and we're going to do – it's going to be a little bit different than maybe what you're used to, or expecting maybe. I'm going to ask Mr. John Grimes, the Honorable John Grimes, to join me here in a second. And it is the first time that he and I have actually appeared on a public stage together. However, it is not the first time that we've either met or worked together or handled the issues that confront us today.

As we were going through the confirmation process together last year, we talked several times about the business of how it was easy for so many folks to point to a rift between DOD and the intelligence community as an excuse for not doing something or as a reason or an inhibitor, and he and I pledged as we were going through the confirmation processes separately in 2005 that we would take that excuse off the table. We saw that as an artificiality and one not productive either for the country, the intelligence community, DOD, or the other partners that we've got in the business of working the nation's business.

And so not only is Mr. Grimes here, but we've also got several folks from across various government agencies that I think will contribute to our discussion. Interact, challenge us, probe. This is

important. We don't need to be dodging issues; we need to be addressing them head on in a forthright, direct, professional manner. It's okay to disagree. As a matter of fact, it's healthy many times. But it is not healthy not to move forward, not to make progress. And so I'm very pleased that Mr. Grimes is where he is and I am where I am because we're looking forward to doing great things together.

As many of you know, Mr. Grimes has been around this business for a long time. I think they invented dirt when he started working the IT business. He has got a great career that has spanned many organizations, to include the White House, the Pentagon several times. He was in the Air Force, and he was temporarily insane for a period of his life when he was part of the Army, but he recovered, and it is indeed my pleasure to welcome up to the stage the Honorable John Grimes. If you would, sir. (Applause.)

Okay, thanks. Thank you very much. I appreciate it. And if you would have a seat, I'm going to spend about five or six minutes outlining a couple of priorities for the intel community. Mr. Grimes will then come up and do the same thing for DOD. And then I believe we have cards running out through the audience, and we're going to filter those cards up here and he and I will spend the majority of our time answering your questions directly.

The business about intelligence is the business about values and how you carry out values. The business is about making intelligence better for the nation; it is not about making IT better. The business about IT is in fact getting a job done. That's what we need to be about. We need to be focused on that. The values that we're looking to instill, from our perspective, are speed, agility and transparency. We believe that those are the keys to sharing information.

As I go around the community, people tell me, we're really all for you succeeding to get those other guys to do what we're doing. Oh, yeah, I believe that those guys ought to be sharing information; I don't know that I should. Those are the kinds of things we need to work on.

We embarked on several things, most of them jointly with the Department of Defense. Most of you have heard about the certification and accreditation reengineering efforts. We're going to brief you on some of that. That is working out very well. We've got tremendous involvement from across the community: DOD, other agencies, Department of Homeland Security, DOJ, Department of State. Just about anybody you can think of across the government is helping us – the NIS very much involved in that.

The Green and Gold teams right now are going through their paces. We'll give you a little update on that, and we do believe that by the end of the year that we're going to come out with actionable direction ahead in how we're going to reengineer the certification and accreditation – in essence, the business of bringing innovation into our community to better serve intelligence and the needs of the nation.

You'll see many joint things. Mr. Grimes and us have worked very hard to work on creating joint offices. The first one we created was the Joint Cross Domain Office, which was set up up near Fort Meade, and we've got some session breakouts on that. The leadership of that organization is here and present as well.

We've made some breakthroughs with our allies in sharing information on classified systems. Again, I can't go into many more details than that, but we've had some things that I think are really breakthrough activities, and those breakthrough activities have had some very high-powered, short-term, war-fighting implications for where allies and U.S. troops serve together, and we can point to those successes as elements of information sharing that are fundamentally different than things that we've done before.

The business about IT management, the business about data structures, expanding the architecture work to be more than just infrastructure. The "I" in CIO stands for information; it doesn't stand for infrastructure. Sometimes I like to think the "I" stands for innovation. Sometimes I like to think the "I" stands for intelligence. I just hope it doesn't stand for idiot. But in any event, we've laid out an aggressive program. I'm not going to go into any more detail because you will see that program laid out throughout the rest of the week.

So, if I could turn it over to John Grimes and let him lead with his few remarks, and then we will answer your questions.

Sir?

JOHN GRIMES: Thanks, Dale.

MR. MEYERROSE: You bet.

MR. GRIMES: I wasn't sure of the format, and these lights up here, they blind me, but Dale made a couple of comments there in the beginning that I would hope most of you understand that we are joined at the hips – using his term – that since both of us have been in about nine months, compare a lot of notes. Now, we don't do it every day, but the staff are. We're very committed to that. It's important to the nation.

This conference, which I was excited about when I saw the agenda – and of course information sharing is the basis of everything we do. I mean, our whole life – as long as I've had any career – we didn't always call it information sharing, but communication is just information sharing. In fact, he mentioned the Army. When I was at Fort Huachauca we started the Information Systems Command, one of the first times they recognized in the Signal Corps that information was critical.

I'm going to tell you a couple of other things here in a few minutes on a chart because we're being challenged today – or I'm being challenged today on content and my role, or the CIO's role. But the department recognized long before I got back – because I retired about 13 years ago and somehow got convinced to come back, but – it was kind of dumb at this point in my career. But they recognized transformation was critical in the department at many areas, but the most critical part, the keystone of that – or cornerstone of that was transformation was called netcentricy. And my predecessor, who many of you I think will recognize, Dr. John Stenbit put in place a way forward, and I would call that innovation, where he was taking the technologies, whether it was transport, the applications, the fusion, and he put this together.

Now, let me tell you the interesting part about that. He wrote this very nice vision and got a buy-in. The buy-in was such that it shows up in the national military strategy, it shows up in their strategic planning, it showed up in the QDR. Well, many of you will know that a vision is pretty easy to write. Now I'm the guy that's saddled with implementation of that vision, and let me tell you, it's hard. It gives me a headache every day: things like GIG, the Global Information Grid; bandwidth expansion, which has been a successful program for the transport layer. TSAT is the satellite system which the community – in fact, the community is using the GIG in a big way, and I believe you're the largest users of the GIG. And then TSAT, which is pushing technology and won't be available until about 2014, but we're doing a lot of work in that area – very expensive program.

The one that is really causing me grief is the JTRS. That's the Joint Tactical Radio System. And we've had a lot of problems because we started a program back in about 1996 with our eyes closed in the industry – and this is where I fault industry a little bit. They could promise us the world but they haven't delivered a damn thing – I'll just tell you that right now – in JTRS. And we've had to change the requirements way back. We're now going to have a radio operator that can do the ground environment and the sharing and the netting that we would have at the edge. And we look at it as power to the edge because everything we do is focused on the war fighter now. Everything is that. And so the edge is the area.

In fact, I just came up here yesterday from the Defense Science Board down in Irvine, California, which did a summer study – each year they do two weeks. One of the major issues and the problems that the commanders in the field have is the information sharing across not only the joint community but also with the coalition and allied partners. And I was out in the theater back in March for two weeks and heard the same thing. As Dale mentioned, the Cross Domain Solution Office has been set up. The community office is to focus on that because we had all these initiatives out there, some of them not even clear – gave us some holes for our adversaries to have access to our network, which has concerned us. We think that this office is getting its arms around and will shrink that up, but that was a big issue when I was out there in the theater.

The second one that is hitting us very hard by our commanders and that is the data strategy – the community of interest. So they will interoperate. When I was in the department in the early '90s it was an initiative under now DCA – D-C-A – to set up a centralized data standards group. It kind of fell apart because it was top down. What they've done – again, it was started prior to my showing up on the scene – working with a community of interest and let them generate their particular area of responsibility, and it's really take hold big time, and we're quite excited about that now. We've got to do this across the main sharing. And some of you might have heard of Mike Krieger who is out leading that effort. But he's not doing it alone; the whole community is involved with him. We think we're on the right track. But that also adds to this information sharing which is so essential.

Since 9/11 I've participated on the Defense Science Board as just a private citizen, looking at the issues of sharing information and what happened, and let me tell you four or five things that came out of that, which now I sit on the deputy's committee with Dale and some other folks on information sharing based on the 9/11. But this goes back to 2002.

The number-one issue that was touched upon is culture. Culture. I mean, that is an issue we ran. We visited; we were briefed over a year looking at this issue of information sharing. First it was the law

enforcement and the IC community, or the intelligence community. We saw some very interesting things – in fact, we talked a little bit about this yesterday evening – where the culture was such that the, oh boy, the lower levels were comparing information after 7:00 in the evening until 7:00 the next morning about when the hierarchy came in the next morning, but when the hierarchy came in the next morning, everything clamped down. Well, that's a culture issue. We saw culture issues at the local level between the FBI, the city policy department and the firemen. So a lot of the information sharing issues were from the culture.

The technology issues, yes, have somewhat been a problem, but not near as much as we think the culture has been, and we're going to talk a little bit on – in fact, one of the things that I'm up against right now is in the department where they were trying to drive me into being the content manager. Now, the CIO definitely plays a critical role in helping the owners of that, whether you're command and control, intelligence, or business systems. And that's kind about the way we look at things in the macro sense, the war fighter or the C-2 systems, the intelligence systems, and our business systems. National leadership of course is the president and the things we do, especially go on emergency operations, and then we have our nontraditional partners and emergency ops like Katrina.

So we are really debating this and how much we get involved as a CIO. And I can show you – in fact, what I've done in the center of that chart – I made this chart up for the Defense Science Board, and after reading Dale's agenda I said, well, I'm just going to show that to you. And basically it comes down to CONOPS where the operators many times do not understand how to connect to each other or what to share with each other. They have application problems, the toolboxes, and for example, the department issued or awarded a contract for a department enterprise-wide collaborative tool. And many times, the users do not understand those tools, so we have to, as enablers, to do that.

The classification – that's another culture issue. But slowly, the markings are coming down. You mentioned some stuff we're starting to share in the classified area on SIPR – I won't get into that – but with our allies. Certification and accreditation is very critical, and Dale, I give him credit for really getting behind that, but we're working that one hard. And of course, most of you know the privacy issue. Anything we do – I don't care where I go, whether we're in a DC deputies meeting or any of the others, you have the lawyers there to protect the fourth.

So then it comes down, lastly, to the TTPs, what we used to call SOPs of how they operate together. So there is a role for us. Now, we looked again at netcentricity of the network and those technologies. And I mentioned the transport layer, but the big layer is the netcentric enterprise services. And the collaborative tool was just one of many tools. And of course, we're using SOA – service oriented architectures – to start separating the data from the applications and putting it out there on the net. And of course, the only way you do that is to have the community of interest data strategy, which we're working on.

So all that is coming together. We're working that as a team. And so, I'm going to kind of stop there. I think that my fifteen minutes is up. And I would be glad to answer any questions. And I just think this is really a magnificent opportunity that I didn't envision when I first was asked to come to it, so thank you, Mark, very much.

MR. MEYERROSE: Good, thank you, John. (Applause.)

Okay, if I can get Mr. Russell to come back up here, and he will orchestrate control of questions. While he's doing that, I've got a request of everyone. I think all of us have personal friends either in uniform, government service, or in industry stationed somewhere around the world in harm's way, and so tonight at the bar or at dinner or whatever, how everybody telling at least one war story about one of our comrades and colleagues who are over doing the nation's bidding and putting their lives at risk. And I ask you to always keep them in your thoughts and prayers. Mr. Russell?

QUESTION: All right, sir, we have a number of questions that have come from the audience. Some were actually done in multiple areas. But as I get started, if you have a cell phone or a pager or Blackberry, either put it on manner mode or get it turned off. The first question from the audience – the CNA process was an excellent first choice for reengineering. What other reengineering efforts are envisioned for 2007?

MR. MEYERROSE: Okay, I think I'll go ahead and take the first shot at that, and then Mr. Grimes can intone. I think the business about pushing jointness – and you're going to hear us say that time and time again, this business about pushing joinness – when it comes to data standards, which Mr. Grimes talked about in his remarks, and ID management – now most of us think of ID management as password and ID account; we're thinking broader than that. There are all kinds of entities that need IDs in a netcentric environment. They can be organizations.

You know, that business about managing information can be an ID management issue. And I see the element of ID management at the crux of creating trusted information exchange. And as we go to more and more netcetntric environment, web-enabled, less point-to-point, less controlled instances of where we limit or descope the transmission of things, ID management becomes even more important. As some of you have heard me say several times, the goal is not to have secrets; the goal is to use secrets for the nation's purposes. And the broadest audience is what we need to use those things for. That does not mean that you disregard security; that does not mean that you don't care who has the information, all those kinds of things. You do. So the things that we can do to help enable that trusted information exchange environment – surrounding ID management and data are the next areas of interest I think you'll see us push on, and again, push jointly.

MR. GRIMES: Yeah, let me just pick up on that last part that you made. Unfortunately, we have individuals out there in the communities on both sides or all around that think they own the information. They do not own the information. They're just stewards of that information of the United States government and should be used as appropriately as possible. And that's another culture issue.

Now, to follow up also, it turns out – and we have not compared notes – my emphasis – and I'm going to be soon selecting a deputy assistant secretary for network and information assurance that I want to focus on ID management, biometrics, that whole area, because if he gets you in trouble if we're not going together on the standards of how we do that – and of course, we've got PKI and the CAC cards as our early capabilities. But I'm going to tell you, it's not going to be long for those that are familiar what the threats are, that's not going to do the job. And we are very concerned today of what's happening in our networks – the unclassified networks, that is, right at the moment – to threats. So this is another hopefully way for at least interim is to push the PKI and CAC card. But identity management is the area

that I think we all are. Now that all fits under what I consider the IA umbrella, so we'll work that one very hard in the coming year.

MR MEYERROSE: If I could re-engage on a point that Mike made that I think many in this audience need to realize, John talked about biometrics. Biometrics means different things to different folks. To a lot of the folks in this crowd, it's the business about proving who you are. But biometrics in the intelligence business, there are intelligence functions that are done with biometrics and we need to remember that, and then there are S&T functions done by biometrics. And so as we work to issue a biometrics across the intelligence community, we're working in all three of those areas. So don't think of that in narrow terms, but in more broad terms. Thank you, Rich.

QUESTION: All right, sir.

MR. MEYERROSE: You know, you had the time while we were talking to sort through the cards.

QUESTION: Got them, sir. As a follow-on to that, many of the organizations that compose DOD and the IC have multiple business and technical architectures. What are the things done to bring synergy to those architectures and promote information sharing?

MR. MEYERROSE: In the intelligence community, we've in fact created an organization organized around that, set it up by Mr. Steve Sohen (sp). He's back in Washington, D.C. He missed the meeting so he got stuck back there, didn't get to come out to Denver. In the past, we have considered the business about architectures in the intelligence business as being infrastructure supporting and narrowed to that. So the business about the integrated collection architecture in the past would not be considered a part of our architectural work. The business about our human resources architecture would not be considered a part of our architectural work. And in fact, all of those are a part of the architectural work. We have worked with DOD in several niche areas, which we're trying to grow those into broader areas.

And both John and I serve on the federal CIO council along with Jim Van Derhof and a couple of the other CIOs that you'll meet here this week under OMB's guidance for the federated architecture structure. And there are certain standards that we've committed to that we're in the process of bridging all of our legacy efforts over into that to make sure that we use common terms, common frames of reference, those kinds of things.

I think the thing to recognize about architectures is so much of the architectural work of the federal government has been shelfware. We have spent billions of dollars on nice prints that occupy 3-ring binders, and while that may be of historical significance, it's not relevant to doing things in the future. And so it's our goal to make the business about architecture a dynamic, living organism that helps us sort through priorities, helps us with programmatic and budgetary decisions, that helps us tie together technical underpinnings, that helps us sort through processes and process engineering and those kinds of things. And so that's the philosophy that you'll see us take with architecture.

MR. GRIMES: Yeah, I think that the department again has embarked on a thing called the gig architecture, which is a macro architecture in how all these services come together. And as Dale indicated before, originally, back when he and I working at the DOD thing early was always at the

infrastructure level, the calm part if you will. Or today, it's much broader than that. It enforces the apps, and a lot of focus on that. Within that though, we have a major program on the national – I'm sorry – the netcentric command and control of how we all go all the way down to the war fighter. And we're trying to get our arms around it. So you've got to get your arms around some pieces of it. But in the larger sense, we are working together so that the common interface points will take place and we initially can exchange. Eventually, if we go to netcentricity and get the stuff out of the net, we don't care where it is as we have some of the new techniques for tagging and tracking. It's going to help us, and it's a must. We've go to, because what's happening inside the net today.

QUESTION: All right. We had a number of questions related to software development and streamlining of system softwares and technologies, so while information sharing is occurring with many, similar software development, portal efforts, such things as a common collaborative tool are under consideration in many agencies. How can the DNI and the DOD work together to eliminate the repetitive nature of these activities to provide lower IT operating costs and a singular capability across the community?

MR. MEYERROSE: Well, I think there are two things to consider in this regard. In the intelligence business in the past, we've been pretty insistent upon tailoring software, building it, making it God. And there have been good reasons for that in the past. But that's hugely expensive. I don't think we ever fully consider the lifecycle costs of development of tailored software, particularly when you're looking at the business of sustaining it – what it takes to sustain something. You know, I've been part of hundreds of discussions over the years of somebody coming in saying we need to do this; we need to do that; and of course, it's on the business of fielding it. It's not in the business of sustaining it.

And it's my judgment that we in the intel community – and John can speak for DOD – that we need to leverage more of the commercial, off-the-shelf stuff. We need to have less tailored software. Every locally devised line of code is a stovepipe to the rest of the world. Now, that doesn't mean we can eliminate it necessarily, but we need to change our orientation that says if there is something that someone else does that we can leverage, we need to do that. We don't have to have the pride of authorship of designing our own. And so I try and extol our folks, if you think you need to write your own pearl script, think again. What can we use that has the most wide applicability for use and reuse?

Now, that brings in other issues. That brings in the issues of offshore development. That brings in the issues of configuration control. There are other issues that attendant to that, but just because those are hard issues doesn't mean I think we need to turn away from that, because I think that is a strategy, which will help focus more and more of our resources to the business of making intelligence better.

The second area of thought that I think this is important is – and I get this from industry all the time – we go to agency A; we spend months working with agency A getting an okay to use the particular application or whatever; and then when we go to agency B, agency B doesn't recognize the work agency A has already done. We're working to change that. That is part of the certification, accreditation, reengineering. Once you have a good housekeeping seal of approval of a certain level, in which we use common criteria, then that approval will be applicable across agencies. And again, we've got a lot of spadework to do in this particular area right now, but that's our goal.

MR. GRIMES: Actually, we're on that same path. One of the major findings and recommendations of the Defense Science Board – and by the way, those who are not familiar with the Defense Science Board, these are some of the foremost minds of the nation, and they touched upon everything that you just talked about, and said that you should not be out there modifying cuts to get you in trouble and the turnover, the inoperability, the configuration management. Issues like offshore, too, is a major concern. So we're embarked and we have been embarked on – because I'm the MDA; I'm the guy that approves a lot of these programs now. Herein lies a problem that you were talking about.

In the Department of Defense, as you know, we have been living off of supplemental funding for the last four years, I guess it is – big, big bucks. Those dollars float right down into the military units at a division level. These folks – the contractors are showing up, new contractors are showing up and we have had a couple of real hiccups in the theater where a division and a rotation goes in, brought in tools perhaps that was not compatible with what was already there – it was embedded there – caused major disconnects.

It's hard for us sitting in Washington to get a hand on that, even when you write all of the policy, and we have smart people out there in the theater – the captains, lieutenants, even sergeants that even write some code and put programs – and so we have had some real hiccups when this happens. We had – just I guess it was back in March when I was over there – one division came out of Fort Hood replacing another. And all of the sudden they brought in different types of tools, collaborative tools being one of them, and it did not fit on fusion. Well, you know, there is a tool we have been using out there on horizontal fusion.

So it is a problem to get our arms around. When the war is over, or the wars are over, hopefully that we'll get a better grasp of that, but supplementals have really hurt us on the proliferation of these – probably got standard tools, so –

QUESTION: Okay, to shift gears just a bit, a number of questions came in relative to sharing with our coalition partners, allied partners, the commonwealth. And they are both related to culture and policy. And the DNI recently had a decision to allow commonwealth partners to sell for credit their networks, their sovereign networks.

However, there seems to be an opinion on the part of some designated crediting authorities here in the U.S. that nothing has actually changed, that those sovereign networks containing U.S. intel must still undergo the same technical CNA that we use here for our own systems. And so that is seen as a significant cultural challenge, as well as the issue of how we overcome the no-foreign challenge with regard to intelligence. Could you comment on those two?

MR. MEYERROSE: Sure. If we had another venue in a classified area, I could prove to you that it has in fact changed, and there has been substantial change over the last few months in the business about how we do things with allies and coalition folks. I think there is something important to remember, and that is not everything is an intelligence equation. The opening up of some of those venues and avenues that we have undertaken recently were done for operational reasons.

Intelligence was getting to the places it needed to get, and so it was not a question about where you – was someone getting the right intelligence, as were they able to operate in the operational environment, and that is what was the driving force on those sets of issues.

In that regard, we in the intelligence business need to remember that what we do is needed by people outside of the intelligence business. Whether it is early warning, whether it is analysis, no matter what it is, the product we create need to go beyond the intelligence business, needs to be used by the operational element, needs to be used by other parts of the government, needs to be used by state and local – and again, we have got some discussions set up in this conference to work on that.

And so to say that any network that has got an intelligence pass on it, information on it, has to be handled a certain way – I think is a little bit restrictive and maybe somewhat naïve. And so, again, I'm not advocate of being careless; I'm not an advocate of dropping things that put things at risk. But our approach that says if one iota of intelligence shows up on this network then we have got to have an entire new set of rules to put in force I don't think is helpful. As a matter of fact I think it's counterproductive.

MR. GRIMES: I have not been involved in any of the accreditation like that, but I would like to pick up on a point that you were making on who the customer is for all of this information, whether it's intel or otherwise.

Let me tell you something that has happened in the theater over the last year with some of the senior commanders. In fact, I head one three-star Air Force general who says, I don't need any more ISR; what I need is op intel integrated in how that is collected. And let me give you an example. He happened to be flying an – he was in a – he was in Kosovo – he uses it as an example. By the way, General Abizaid, who is the CENTCOM commander is saying the same thing, but this is an example.

You know, I have – there is a flight that went out and found some sands in a canyon, but they ran out of gas and had to come back. And this general is – he was not a general then; he was a colonel – going out of his flight, the information never got exchanged. It happened to be these airplanes didn't have quick radios in them.

So he goes out there, but the information of what those – the first flight had seen never got back to this other flight that was going up. And they are using that as an example on op intel. What is happening on the scene right now, especially in IEDs over in the theater – so you're going to hear more and more about optel. And ISR is okay and needed in the longer fight, but the immediate operator, the customer needs information one what happening on this scene now. And you are going to hear more on that in our community.

QUESTION: Okay. And also, to both you, how do you see the role of domestic law enforcement and that community in relation to intelligence and defense information systems, especially at the state and local government levels dealing with independent legal authorities or challenges?

MR. MEYERROSE: There are a lot of things that is new ground for us as a country in this particular regard. You know, it seems kind of counterintuitive, but if you think about it, we have created a Defense Department and military apparatus in the past not to defend the United States, per se, but to exert U.S. policy overseas. And so 9/11 sort of gave us a little bit of different perspective. It says that

there is a role. And that role has to be balanced. And the business about net centricity and things like that brings into questions things like U.S. persons and what constitutes a U.S. person and what rights does that constitute. And we are very, very cognizant of that, and we want to pay close attention to those discussions to ensure that we fall within the bounds of what is legal and constitutional.

But as some of you know, I was in U.S. Northern Command. I helped stand up that command a couple of years ago, three years ago – almost four. I don't do math in public very well. And the element about you – one responds to an event-based, event-driven event somewhere in the United States to where the United States military has capability that is not resonant in a state or local activity. The classic example is what NORAD does associated with being able to intercept an airplane at 35,000 feet. I think the United States military is about the only entity in America that can intercept another airplane at 35,000 feet and do something about it.

And so think about how we as Americans have grown accustomed to that idea that says U.S. military and cross-border things with Canada and Mexico in fact – working through some of those things – that might be some if the things you might want to talk to Lieutenant General Rick Finley when he comes and speaks to you later – are all new issues. And so we are having to work through those very, very carefully.

But just because they are hard problems doesn't mean you need to avoid them. And just because we looked at this issue back in 1984 and we came to the conclusion, well, maybe 1984 wasn't the right time and we've got to relook at the issue again because the parameters have changed – you know, look how accepting we are as Americans when threat levels change in airports and things like that. You know, think about what our attitude would have been on that prior to 9/11. It would have been one of indignance – one of being indignant about what we were being asked to do.

And so I think that's a constantly shifting set of values that we need to be plugged into the political elements and, again, realize that folks other than the intelligence community use things. And so things like tear lines, things like – and tear lines can also be not only things with classifications but also with U.S. persons and those kinds of things.

MR. GRIMES: In the past week there has been about three major meetings involving the president and the deputy secretary – I'm sorry, the secretary and the staff on these issues. One, the Department of Defense is not a law enforcement agency. Of course, one of the reasons that the military has had such a high level of prestige with the American population, it's never been in that role. However, it is in a supportive role, and it's, again, really – well, we had a couple of instances where the National Guard was activated – federalized, but the counter-drug program back in '89 when the Congress passed a law that the Department of Defense had to support the counter-drug – and I was involved in the initial part of that – but we didn't do any law enforcement. The Coast Guard did that off our Navy ships; the Army, working the borders.

So we're very sensitive about the role the Department of Defense does, and domestic law enforcement. So the secretary makes it clear. And for those that – I would appreciate it that – you know, we've got 6,000 guards on the border now assisting, and the secretary makes sure that that cost is not going to come out of the top line of the Department of Defense, and it's going to come out of Homeland

Security. So that's the sensitivity about the department looking like it's in the law enforcement business. So we are not in the law enforcement business.

QUESTION: Okay, thank you. Shifting gears just a bit, traditionally there has been a rift between open-source information, or intelligence, and the traditional classified intelligence streams of information. How do you see this situation changing as we move forward into the future?

MR. MEYERROSE: I don't know that I would characterize it as a rift. Again, let's get back to our values. For 50 years it's my judgment that in the intelligence business we took the view that if information was classified, it was important; if it was unclassified, it was unimportant. Now, that's kind of being a little glib and taking things down maybe a level or two without full explanation, but thing about what our actions were, you know. And in fact, I say to people today, if it's not on my classified network, it's not important.

I think the thing that we need – again, need to remember is that the business about open-source and unclassified elements give meaning and structure to what we do in the classified world. What you're talking about is information, facts, data, whatever. Whether or not it's classified or unclassified is the means of collection, and nothing else. And so if you came to know it through the Internet or the Encyclopedia Britannica or Goode's World Atlas, or something like that, that somehow had a lesser value than the fact that we came through information via collection means.

And so I think we're, again, in the process of culture shifting our values. And we have an open-source center under the oversight of the DNI. The executive agent happens to be the agency. And I think that's significant because, again, our concept about how we think of ourselves in the past is something that we're in the process of reviewing. And so, you know, the business of – we need to figure out how to come up with a value of information that's not solely based upon means of collection. If we have a coastal city in the United States that has a radiological bomb in it, I think the geocoordinates of where that bomb is and the geocoordinates of response forces and things like that are probably the most valuable information you can have, and none of those may come from national collection means.

So, again, I'm not talking about devaluing the business of collection because that is central to who we are in many respects, but it's the business of how we attribute value to information in general, and that's what I see as a suggestion.

MR. GRIMES: You know, a lot of this is self-serving when people don't want to – especially in their community – and I'll give an example. Back when it was the Defense Mapping Agency and NIMA, nobody was going to use any commercial products. Today it is – and especially over the U.S. because the NRO – our assets are not set up to be over U.S. – not that it can't be used, but that was not the purpose. But today is an example how we use those commercial products.

Well, the same thing has happened in the open-sources area, and I can tell you, when I was on the NSC back in the mid-'80s, we did some of the early open-source work, and it was quite interesting – when I say open source, we'd look at newspapers and CNN and got some awful good aggregation that's the word they use, aggregation – and you could get some pretty good signals. And I can tell you, on 9/11 they've gone back and looked at open sources, and a lot would have been revealed if that had been used in the community.

QUESTION: Okay, as a final question, could you please expand on the evolving relationships, in both mission and scope, between the DNI, DISA, and intelligence components of the Department of Defense such as DIA, NGA and others?

MR. MEYERROSE: Sure. If I could just expand that question just a little bit more – let's not limit it just to DOD and DNI. You know, DHS, DOJ, Department of State, FBI, HHS, across the board. I think there is a parallel.

The reason why DOD and DNI are so closely linked together is that most of the intelligence resources are in the Department of Defense. The reason why we're so closely linked together is because nine of the intelligence agencies – nine of the 16 intelligence agencies have Title 10 and Title 50 responsibilities associated with the Department of Defense. And so while that's the major focus and while John and I are committed to make that a strong partnership of synergy rather than a frictionous one that is divisive, the business about inclusion across the federal government, and with nongovernmental agencies and things like that, the philosophy has got to be the same. The business about being joint has got to be a similar kind of approach. And so we're trying to do that across the board.

Later in this conference, Ambassador Ted McNamara, who is the program manager for the information sharing environment, who is the focal point for the United States government in working across that wide spectrum, is going to join us, and I think you'll see in his remarks the amount of interface that we're really talking about.

There is nothing like good, open lines of communication to resolve issues. The business about – there is not one single thing that I am the least bit reticent of picking up the phone and calling John Grimes and saying, okay, this is the indication I got, this is what I think; what indication do you have and what do you think? And there has been no instance to date – not one little one, not one big one – where we've had that interface that he and I differed on how we ought to go forward.

But it's not just enough for John and Dale to do this. You know, our staffs have to do it, and down through the rank and file of people who do the work every day, who are accountable for doing the nation's bidding and are the subject matter experts in many things. And so we've got to work on a myriad of levels to make sure that the business of our intentions manifest themselves in the right outcome. And this is about outcomes: Do we have the right outcomes? And if we're not getting the right outcomes, then we need to change the input, and that's what we're committed to do.

MR. GRIMES: I have, every two months, a meeting with all my CIOs and C-4 three stars, and I invite him to sit at the table, and he can tell you that we talk about adopting the best, whether it's from them or the Army. For example, the army's AKO has been adopted for the defense, but that sharing at that level – many times, you know, we're in our office, we're dwelling on our own internal problems; we don't have time, but when you have these kinds of venues where you share – and DISA, by the way, works for me – General Croom, and he in particular has been very active in this adopt-and-share technologies through the three services and the joint staff. So that is one of the dynamics that's taking place.

The last one I want to just mention back again – you mentioned Title 10, Title 50, and of course Title 40 is where I get my authorities, more authorities then actually with Title 10 under the Clinger-Cohen and the national security systems that's included in there, and that's where I get involved in the information defense, or IEAA. The stuff is done by Dick Shaffer and company down at Fort Meade, and I kind of have an oversight of that responsibility. And of course it is a Title 50, and then we have a Title 10 role too.

So we have to sort that out, and some of that goes back to money too, but in the main, those barriers have really come down, and within the NSA they have embarked on – they don't use the word anymore, but it's blending and looking at the offensive and defensive, and a lot of work is going on in that area, to include the role that General Cartwright has, and General Croom, as the commander of the Joint Task Force for Global Network Operations that looks over all the GIG worldwide, which you're a customer of, and looking at content – in other words, attack. So that's work with the NTOC (ph) at the NSA.

So a lot of this stuff is coming together. Why is it coming together? It's these personal contacts and those of us that have kind been out there in the theater. It tells you that we're getting old. (Laughter.)

MR. MEYERROSE: Well, I'd like to close by – John, thank you very much for honoring us with your presence, your friendship, and we appreciate your participation. It has, I think, helped this conference.

We have a highlight coming up after the break. Dr. Tom Fingar, who is the Deputy Director of National Intelligence for Analysis, is going to address us, and I know that none of you will want to miss that.

So, John, again, thank you very, very much. Please accept this small token of our appreciation. And, yes, it goes underneath the dollar limit. (Laughter.) (Applause.)

(END)