SPEAKER:

DR. THOMAS FINGAR

DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE FOR ANALYSIS & CHAIRMAN, NATIONAL INTELLIGENCE COUNCIL

AUGUST 21, 2006

DR. THOMAS FINGAR: Thank you. Thank you all for coming. I am absolutely thrilled that Dale Meyerrose has given me this opportunity to speak directly to those of you without whom I cannot succeed in my mission of transforming analysis. I have the perhaps unenviable job of being the tail that wags the dog. Analysis in the intelligence community is one of the smaller components, less than 20 percent by people, a lot less than that by budget. Admittedly, after 40 years as an analyst, I have a bias. But I approach the task and the transformation from the perspective of "It isn't intelligence until it has been processed through the brain of an analyst. It's just data." And we are awash in data. We don't have enough analytical brains to meet all of the challenges. We have to rely on technology. We have to rely on collaboration, and that requires information sharing. It's not in the nice to do category; it's in the absolutely necessary to do.

So what I'm going to try and do this morning – reverting to my old professorial mode by talking at you for quite a while – is to lay out some of the things we're trying to do in analysis. And the "we" here is not Tom Fingar and his little staff; it's not ODNI; it is the collection of analysts and analytic components in all of the agencies of our community. Many of us have worked together for decades. Ideas that I will articulate today, I have stolen without shame from many of my colleagues, and they prod me regularly to adjust the vision to meet our collective objectives.

What are those objectives? One is to transform the analytic component of our community from a federation of agencies, or a collection of feudal baronies, into a community of analysts, professionals dedicated to providing the best and most timely, most accurate, most useful analytic insights to all of the customers we serve – policymakers, war fighters, and first responders; to do this in ways that draw upon

the collective strength we have inside the community and the incredible amounts of knowledge that are available outside the IC, outside the U.S. government, and even outside the United States.

Central to all of this is collaboration. I always use the word collaborations rather than cooperation. Cooperation is something we make people do: Play nice in the sandbox. You will come to this coordination meeting. That's not good enough. Collaboration must be something people are excited to do; do without thinking about; do in ways that are invisible or transparent; do because they recognize it leads to better insights, and more timely responses.

I'm hopeful that this vision will excite some of you. I anticipate it may frighten others, because what we're talking about here requires changes that are more revolutionary than evolutionary. We can't go back to the future, the halcyon days of yore when the intelligence community functioned as a thoroughly integrated if completely mythical establishment, when we moved from breakthrough discovery to breakthrough discovery. The world is very different; the challenges are very different, and incremental change won't get us there. Indeed, we probably have used marginal improvements as effectively and as thoroughly as is possible. There's not much more that we can wring out of doing it the old way, but doing it a little better or a little more efficiently.

Radical change isn't just imperative; it's also possible, which is a happy coincidence. We could not have done this five years ago. Despite the recognition by an awful lot of the professionals in the community, and a lot of the gadflies outside of our community, that we needed to do things differently, it sadly took the tragedy of 9/11, the wakeup call that that entailed, and the fiasco of the National Intelligence Estimate on Iraq WMD to create an opportunity, the first in two generations, to really transform the way we do business. If we don't take advantage of this opportunity, shame on us. We've got congressional encouragement and support; we have public expectations that we will do it differently; and most importantly of all, we have experienced professionals in the community who "get it" and understand that we have the most to contribute and the biggest professional stake in taking advantage of these opportunities.

But let me dwell for a moment on some of the reasons – and it's a small subset – that we have to do things differently; we have to collaborate; we have to share. One is the articulation of the blindingly obvious: the explosive growth in the amount of information that is out there. This reflects the recognition that open sources – the information that the rest of the world uses all time – is important for us to look at. There is a lot more open source material than in the past. The introduction mentioned my China background. It recalled for me a project that I did in 1975, which was to compile a list and what we knew about Chinese periodical publications. We didn't necessarily have them, but we had some reason to believe they existed. There were 73 publications on that list. Now there are tens of thousands of Chinese publications. China is an exceptionally large country, but the basic phenomenon is repeated in all of what used to be the Soviet world, in much of what used to be referred to as the developing world. There is a lot more information than ever before.

In addition, our collection mechanisms have become vacuum cleaners on steroids. Decades of analysts going to collectors and saying, "I want more," more of what – more of everything; more of whatever you can get. The technical wizards have managed to fulfill our fondest wishes in ways that now leave us screaming uncle. We can't possibly process and manage in the old way the amount of information that we have.

Another reason we have to do things collaboratively is that the scope and the complexity of the issues that we are asked to analyze, which the intelligence community is expected to be able to do by those we support and by our fellow citizens, is far, far broader than it ever was. I remember – imperfectly - a study done near the tail end of the Cold War. We had about 85 percent of our analytic resources devoted to a dozen countries and not many more topics than that. In some ways, it was easy to be very good because we didn't have to look at very many problems. Many dimensions of those problems, but most of the world and most issues were outside our zone of interest. Now, we are as likely to be asked for relationships among individuals scattered around the globe, red lines in the thinking of terrorist organizations, details on tribal, religious, ethnic, or regional cleavages somewhere in Africa, prospects for nationalization of resources in Latin America. These questions are hard.

What makes them particularly difficult is the compression of time. We've all experienced it. Every great laborsaving device seems to make our workday longer, leaving less time for that spare-time activity called life. But the compression of time in the policymaking, war-fighting, first-responder world that we support is such that we are expected to have information and insight on a far broader array of questions. Moreover, we need to have it very quickly in precisely the right tailored format. Otherwise, we become a very expensive irrelevance. If we can't provide information in time for that flight to take off – to pick up on Mr. Grimes' examples – in time for the decision that is being made in the State Department or at an international conference – in time for a governor to make a decision on whether or not to shut down the tourist industry in his or her state because of a threat – we're perceived as not very helpful. So, we've got to respond very quickly. It's no longer simply a matter of saying, "well, they just laid the keel of a submarine. Now they've built it. Now they've launched it. Now they've given it sea trials. Now they've incorporated it into a fleet" with this occurring over the period of time my kids went from kindergarten to college. We were very good at tracking slow-moving developments. Now we must be just as adept at responding to perishable problems and very, very demanding schedules.

Folks don't only want more information on more subjects more quickly; they also want deeper insight. They're not looking for facts. As Secretary Powell used to tell me repeatedly, "I don't need news. I don't need facts. I have a television. I have the Internet. I have a telephone. People tell me lots of facts. I need to know what it means, how important it is, what you think about it." This is insight. And providing meaningful insight to smart and attentive customers who are usually all over the accounts that they are working requires a level of expertise that is beyond that of most individual analysts and indeed is beyond the capacity of most individual agencies or components of the community.

We can't simply follow the old model of coping with information glut by defining ever narrower and narrower portfolios of responsibility and adding more analysts to mine that information. We've got to be a lot smarter about specifying the questions we need to answer? What's going to give us insight into that problem? Where are the fire extinguisher accounts that I need to maintain today in order to ensure that I have the requisite expertise tomorrow? I'm not going to have time for a journey of discovery to figure out who knows something about the subject or to tell collectors to get me information on developments six or eight months ago after a crisis develops. We've got to think about what we do very differently.

To underscore a point I made earlier, incremental adjustments to the way we do things – and here, one of the most important of those things is sharing of information to facilitate collaboration – won't

make it. We can tinker. But if we tinker, we will fail. And failure is about security; it's about expectations; and ultimately, it's about going somewhere else to get services we haven't provided. It's a big challenge. And there are lots of embedded challenges in this. But every challenge has with it an opportunity. And I mean that as an analytical statement, not a Pollyannaish expression of hope.

Let me provide some examples, which I think will illustrate the point. The first is technology. Technology is a force multiplier. You know more about this than I do. My level of technical sophistication is such that my cell phone has 23 functions, 21 of which I do not understand. But you do understand what we can do with information technologies. More to the point, you understand what we could be doing with technology today that we're not doing because of policy, culture, or ingrained habits that impede making full use of our technical capabilities. I'll come back to this point. Others have noted the importance of culture, and I'll come back to it.

The second opportunity here involves the advantages inherent in smart integration – enabling the intelligence community to function as a single enterprise. This is my community of analysts writ large – collectors working together; collectors working with analysts; IT support people, human capital developers. Others have noted this. If we function as an enterprise, take full advantage of inherent opportunities for synergy, for complementarity, we can be even better than we are.

What kinds of challenges are also opportunities? One is redundant effort to review and annotate and file information. We have multiple analysts around the community who look at overlapping – not identical, but overlapping – reports. This is a big problem for some of the accounts that have hundreds of analysts. It's an extraordinarily great problem for those accounts – which are most of them – that have analysts numbering in the single digits or a few dozen or less. If we can minimize that redundancy with a division of labor whereby when somebody reviews a report, has a thought, scribbles an annotation and makes it available to everybody, goes into a common workspace. We shouldn't have to discover over and over that round is a reasonably good shape for wheels. Once should be adequate.

A second example is to take advantage of the fact that the intelligence community has a multiplicity of customers. It has sixteen agencies that have grown up for their own historic reasons serving that multiplicity of customers. They have experts in them with different types of expertise that look at information and problems through the lenses of the people they support. We have, by virtue of the structure of our community, a customer-oriented enterprise with tremendous opportunities for collaboration, for integration, for synergy -- if only we could discover them, if only we could act on them.

The lack of expertise in the community is both a problem and an incentive. We have a demographic profile in our analytic community that looks like the letter J. Some of you have heard me say this. The short leg of that letter J are the wizened veterans who really know a lot because they've been doing what they do for a very long time. By accidents in perfidious personnel systems across the community they have actually been allowed and enabled to stick with subjects long enough to be true experts. The long leg is the 50 percent of my analytic community with five years experience or less. In the middle is the missing generation – those who were not hired because we were downsizing or rightsizing; we had hiring freezes that reflected the peace dividend at the end of the Cold War and so forth. We're going to lose much expertise pretty quickly. We've got to marshal it now to mentor the newer, very, very talented people that have joined our workforce.

We also have to reach outside of the community, taking advantage of expertise and information that is outside the classified realm – the open source world. Much information isn't classified. It's not necessarily better or worse, it's just collected differently. If we're not beginning the search for insight in the open source realm, we are squandering time and money.

The solutions have an obvious – two heads are better than one; many heads are better than two character. But how do we realize that? Everybody recognizes the truth in that aphorism, but how do we actually make it happen? Well, imagine with me for a few moments elements of a better way to do things. And my proposition today is if we can dream it, we can do it. If we can imagine it, we can realize it. So think about the possibility of analysts working in the open, moving away from the monastic scholar in the garret or a cave or stovepipe, beavering away to go, "eureka, I have found it!" And think of an arena in which – back to an example noted earlier – an analyst who makes a judgment about a report – "terrific report because…I give it low credibility because…I think this one is related to a report I saw three months ago; I think this would change the judgment in an analytic product produced somewhere in the community; I think this reinforces something I read in a vernacular newspaper" – whatever it is that he or she observes is accessible to everybody. It's not written on a 3 x 5 card and stuck in a shoebox, or it's not annotated and put in an individual's personal electronic folder and put away. It's out there for others to look at and to react to.

Imagine a community in which collaboration happens naturally, easily, asynchronously, unintentionally, automatically because people change the way they do their own work in ways that make it available to others. So something that is discovered by anybody becomes a universal property of the intelligence community, or at least that subset of the community that is working on the same or related problems. The discovery might be a fact. The discovery might be an insight. The discovery might be an expert working on the problem somewhere in a university or a corporation or an allied liaison service. Imagine a situation in which any product created by an individual analyst – a brainstorming paper, preliminary thoughts, specialized database, a graph, a map – is available to everybody else.

Think about the potential for peer review. If you see early on the thoughts of a colleague you have the chance to say, "that's really stupid" or "that's brilliant" or "have you thought about or why can't you take those same facts and explain them in this way." To begin that process as early as possible by sharing in a virtual workspace – indeed, preferably virtual rather than physical – where insights are available to all, where we evaluate contributions based not on how many dead tress we have devoted to pages of text, but on how many ideas have been tossed into the hopper, how you helped a colleague in the same or another agency, or what new knowledge you have generated about a problem. Have you shared an inside gleaned from a book, an article, a conversation with people outside of the community?

We all know intuitively that this is a good idea. We've got to go beyond, "yeah, it's a good idea, I wish I could do it," and actually make it a reality. And we can make it a reality, but I need your help. This is information sharing and this is dealing with some impediments to information sharing.

I suspect that I may have upset some of you who may be beginning to think, "well, it wouldn't be prudent to have that kind of sharing." I've observed the argument over the last decade that went something as follows – the techie types say, "we can connect anybody to anybody, anywhere, anytime, at any level, all levels of security, and we can share anything." And the security people say "not so fast,

wouldn't be prudent, can't share with those guys. That agency, that organization, is suspect." Well, we have to revisit the need to know and replace the emphasis on "somebody else will determine your need to know" with, "if you need it, you can know it." And nobody knows better than the analyst what he or she needs to know. Ideally for me -- and my ideal I think should be our goal -- every member of the intelligence community should have access to all of the information in the community. I know there are going to be compartmented programs. I know there will be limitations. But our starting point should be that we want to make it all available and then trim back. It should not be to incrementally allow three more people into a compartment or modify the sharing of a particular database or whatever. We need to "just do it."

Those who know me know I tend to use simple bumper sticker ideas from time to time to make an important point. One such deals with the technical side, with Dale's world of accreditation and certification. We need to move very quickly to the point at which when the CIO certifies a system as secure, it's secure – end of discussion. It can go to any agency. It can move any traffic. It doesn't matter how many terminals are hung on this thing. If it's certified, it's secure, and there's no rebuttal. And the analog of this, and the complement of this, is that anybody wearing an intelligence community badge that has been brought in through the same kind of background investigation, given access, and given training in the handling of material should have access to all the information that is on that system. I'm real tired of hearing, "well, the system is secure from point to that point, but how do we know that the person that is going to pull it off that system can be trusted?" We have to trust our security vetting processes.

But to paraphrase Ronald Reagan, trust and verify. We need ways to audit what people look at. We can't be foolish about this. But if we adopt a risk management strategy in the sharing of information, I would argue, we must begin from the standpoint of if you're in the community, you're entitled to the information. You are expected and required to handle it properly, and we will be watching. It's not that hard to develop audit trails to see who is looking at what and what they are doing with it. Watching what people do is a different way of managing risk.

One of the things that needs to be made clear is who is taking the risk. Believe me, I understand the reticence of some of you who are going to throw the switch and grant the access, but want to avoid going to jail or avoid difficulties at performance review times. We have to make clear if the ODNI and the CIO's office have decided something, it's our butt, not yours. If we've instructed you to do this, we will bear the risks and we will take the heat – and things will go wrong. Therefore, we have to do everything we can to mitigate, but mitigate with the presumption that we're going to share, that we're going to collaborate.

Back to the vision – there's a lot more that we can imagine and must make a reality. Imagine for a moment that we could always know what we already know within the intelligence community, what information we already collected, what analyses we have already written, what modifications we have made to judgments reached by colleagues a week, a year, six months ago. It's hard to do that now. Individuals know it. Some agencies know it better than other components. But I submit that the folks on the Hill and our fellow citizens think that at a minimum, we know what we do and we know what we've done. And that we can find what we've done, can compare what we've done, and can modify what we have done. I wish we could do that. There are some steps we can take. You'll hear some of this from Mike Wertheimer later when he speaks about the national intelligence library.

Knowing what we already know enables us to target our efforts onto what we don't know. And an open work environment among analysts provides a vehicle to identify what we do and do not know. What do I not know that I wish I knew – either to answer a question from a customer or to move my own analysis along? An open sharing, I would posit, is often likely to elicit an "oh, we had that same question or similar question a few days or few weeks ago; here's our answer" response. Much of the time that will probably suffice, particularly if we know our colleagues and have confidence in their tradecraft and are used to interacting with them, so that if you get an answer from a colleague in another part of your own agency or from another agency, you have some confidence that it was researched using appropriate tradecraft. If you disagree with it, you'll know why and can challenge it, but move on from there. Or, say, "I've got a similar problem I can't find the answer to. Maybe we ought to work together on defining a gap, which we'll take to the collectors." This will have peer review aspects. It will facilitate prioritization. It will focus what we ask people to collect, not just give me more, but give me information on this subject, which I think you might find in that place using whatever techniques you think are appropriate.

That's some of the imagined ways to collectively know what we don't know. It's not the unknown unknowns. Within the community, it's too easy to assume, "well, the guys over in DIA must be all over that one." "One of the intel service centers is probably working that problem." "It's sort of diplomatic – INR must be doing it." "CIA is responsible for doing everything. They must have people doing it." Maybe; maybe not. But this shouldn't be guesswork. It should be easy to discover and we have to make it easy to discover.

This is more than a dream. A year ago, a rougher version of this idea was a vision, a dream. But we're beginning to move down that road. And we've moved down the road in part because of the collaboration that already exists between Dale and the CIO staff, and the DDNIs for analysis and for collection. But we have identified a number of impediments / opportunities that require going the next step. Let me tell you some of the things we've done.

One is finding out what happens in the community; who does what, and where they are; mapping the community. One of my deputies, John Keefe heads this effort we call mission management. He started out with a simple question – who in the community does what on Iraq? This turned out to be not so easy and took a couple of iterations before people understood the question. It took a couple of iterations to get beyond– "well, we do everything on Iraq; we do important things on Iraq." "Who do you do it for?" "Important customers." "How do you write it up; how do you disseminate it?" "All kinds of ways." It took a while for people to understand what they were being asked, that this was not a report card; that we wanted to know where we have appropriate duplication to ensure alternative, competitive analysis, and where we have yawning gaps that somebody assumed others were looking at it. To go right the bottom line, we discovered a very large community of people acting like eight year-olds playing soccer, bunched around a ball over here and a lot of areas of the field uncovered. As soon as components of the analytic enterprise saw that, they didn't need me to tell them to adjust; they began to adjust to optimize what we're doing. We've now done this for a number of other topics. It's become reasonably routine. We did Hezbollah – the analytic effort against Hezbollah – in a couple of days, very informally, but very efficiently.

One of the things that I am discovering as I do this, since we started out with the high-profile front burner topics – terrorism, Iraq, Iran, China, North Korea – is that I'm reducing the number of

analysts for other topics pretty quickly. My top five topics occupy almost half my analysts. Among the lessons I draw from that are as I get down into the remaining give or take 300 topics that need to be addressed, I can't human wave them; I've got to be real smart and real effective at marshaling, through collaboration, the resources inside and outside of the community. Again, this is not nice to do; it's absolutely imperative, if we're going to come in with insight and understanding of the kind that is expected of us.

Tracking analysts' skills is a decade-old idea. John Gannon came up with the idea for a database of analytic resources. John couldn't get it off the ground because the time was not right. Mark Lowenthal launched it, but again, the timing was not propitious. He got about 20 percent of the analysts in the community in the database. We now think we may be approaching 100 percent. Among the reasons we think we're approaching 100 percent is I suddenly discovered I've got 1,500 more analysts than anybody thought we had before. It's now going to be linked to budget numbers; if an analyst isn't in the database he or she is not in a fundable position. Knowing who is where, what they're working on, how long they have been working on that account, what they used to follow and consider themselves expert on is essential for collaboration and workforce planning. We have used phone numbers and email addresses to produce a phone book of analysts. This is going to be replicated for all other parts of the community. We ought to be able to find our colleagues easily. I need your help and guidance on such things as: do we rely on individuals to create listserv emails and virtual teams, or do we let the technology do it for us? Should we use it to aggregate everybody who said they have worked on Sierra Leone into a prospective virtual team? If we did, we could send it to all analysts with a note saying, "here is what we think the Sierra Leone expert team looks like and here is where members are." I'm not sure that is the best way to create virtual teams and welcome your input.

Tradecraft standards and training – the media, some on the Hill, and the punditocracy regularly flails the analytic community for the Iraq WMD estimate, and as one of those who was responsible for that estimate, we deserve much of the flailing. But they've drawn a trend line through a single data point and proclaimed the analytic community to be keystone cops incapable and incompetent to do anything. That's nonsense. We are much better than that. On our worst day, we're the best in the world. But on our best day, we're falling far short of where we ought to be, can be, and will be with collaboration. I mentioned the library of national intelligence as an example. The basic idea is that any report that gets produced, raw or finished, can be linked up by machines – making it easier for analysts to focus on what they ought to, linking similar things and discarding things that have already been weeded out by other analysts.

The Collaboration Working Group launched by Dale and I nine or ten months ago has yielded bottom-up proposals – one has twelve pages of specific suggestions from the analytic community and the CIO community to enhance collaboration. I like bottom-up; I assume that the collective wisdom of the community trumps whatever cleverness I bring to bear. And we will be paying attention to their proposals and suggestions.

We're about to launch an experiment in producing a National Intelligence Estimate using the Intellipedia. I don't know if it's going to work. It might; it might not. But we're going to try it– it's going to be on Nigeria. Instead of relying on those who can make it to the meeting or happen to be in town at critical junctions to shape it, we will engage any who are knowledgeable and let the Wikipedia process operate. We'll see if it works. We might have to tweak it. We might want to run the regular

process in parallel, as we are running in parallel a number of analytic efforts where we give the same questions to an outside group using open sources as we give the community to work using all of our classified data. Exactly how much better, and on what questions, does classified information yield better insights than what we can produce using unclassified information? There are people that describe this as one of the scariest innovations that I have launched. It shouldn't be scary; it should help analysts to direct their time and attention to where they get the biggest bang for the buck.

We're launching a new peer review online product in science and technology. Again, we will let those who are expert come up with a topic. Their peers review it. That will be transparent. It will get to a point at which it will be formally anointed by the community that produced it.

Identifying meta-data requirements to link and store raw and finished intelligence – we started many, many months ago – Mary Margaret Graham and I asked what it would take to make all collection products look the same, so that SIGINT reports, imagery reports, attaché reports and so forth all had the same format, making it easy to find the point-of-contact; date of information etc. But this raised questions about how to tag analytic products so they could be linked to one another and to raw traffic. A starting point is to have every report carry GIS information, a location, and temporal information, a time. We've been working with Dale's people to develop the standards. We have draft guidance that also addresses sourcing requirement. This is exciting and on the verge of being ready to preview to the community. Again, this will not be a take it or leave it proposition. We need your input to make this go.

We're also going to launch a "geek squad," no disrespect intended. A lot of analysts, not all with as much grey hair as I have, don't realize what IT can do for them, don't realize what you can do for them, and don't think to ask for help that you can provide. We're going to make that easier. Here, we want to invert the old relationship where folks came at the analysts with cell phones with 46 functions, most of which they don't need and don't want. Let's get the return that we can realize now with off-the-shelf software and knowledge that will help me to do my job today. The geek squad can say, "your problem has already been solved" and tell you what you need to do. Another idea is to link the watch centers around the community so that they can produce near real-time updates like some of the networks do. All of this is doable; all of it will run on an IT system and other more sophisticated technological backbones. You're going to have infinitely more ideas on this than any people in my shop are likely to have. We're eager to have your ideas and eager to act on them. If an idea makes sense, we ought to move on it.

This is a call to arms. I realize that I am not the most passionate speaker. I had a boss who once described my emotional range as running from A almost all the way to B. But if we're going to succeed as an intelligence community, we've got to move now. We've got to do those things which we can do and, we must overcome impediments existing only because we've never done it that way. We also must change policies and practice that impede collaboration. One universally condemned around the community is the use of ORCON. If analysts could burn anything at the stake, it would be ORCON. Why do we restrict how we share information within the intelligence community? Why do we live with a caption that denies entire databases to entire agencies if there's one document containing ORCON? This can't be smart. It also can't be necessary. We've got to go after those things that we can go after. We need to identify potential downsides but not be paralyzed by them. Manage the risk, find ways to verify, and get on with it.

Overhauling the institutions, the practices, the biases, and the SOPs that have evolved over six decades of the intelligence community since the last time we had an opportunity to fundamentally remake it is a big challenge. It's a big deal. But it's also doable, and if we don't believe it is doable, we all ought to resign. We have to get on with it. We need your help in the analytic world on information, policy, and standards – our approaches to access control and decisions on how to audit our activities; our new work processes and systems that support them; on ways to do in the IC what advanced actors do in the corporate world. I mentioned the watch centers – if the networks can be on top of developments around the world and update a website every 20 minutes or so, we ought to be able to do that. I'm looking at Carmen Medina; the WIRE is the new CIA product that begins to move in that direction.

A transformation of the kind that we can imagine requires not just analysts changing the way they do things, but collaboration among the IT folks, the CI folks, the human capital folk, and all of the other members of our community. A good idea is a good idea whoever has it. We can't have the "not invented here" problem. We also should not have people holding back because they assume "if I thought of it, surely somebody has thought of this already." Maybe, maybe not – toss it into the hopper. We're eager for this transformation, but we are not rash. There will be disruptions; there will be failures. Hopefully, when we fail – and we're going to fail – we'll do it quick and cheap. Do this a step at a time and learn from the mistakes. Learn from the things that succeed and keep moving. There is no end point for information sharing. There is no end point for collaboration. It will get better, deeper, more productive, require more and more sophisticated IT input, better and better systems. We can do it, folks. I'm absolutely certain we can do it.

As we close, and before I invite any questions you might have, let me thank you, not just for the opportunity, Dale, to be here, for all of you coming in from the exhibits and the coffee breaks and whatnot, to listen to me – but also for what you do every day. The starting point is not zero. We have an incredible capacity to move information around, to store it, to process it, to gather it. This is not a plea to invent something wholly new. It's a call to invest time and effort, and take risks to make what we've got even better. Policymakers understand the importance of intelligence to what they do. Professionals around the community understand we have an opportunity that may be fleeting and want to move on this. That junior workforce, that 50 percent with less than five years experience comes to us with expectations of collaboration that are wildly different than those of us who came in years or decades ago. Another example of necessary to do rather than nice to do is that if we don't make it as easy for them to collaborate with their colleagues inside the community as they are used to collaborating with partners out there in the digital world, we will lose them. And we cannot afford to lose them. We need them to do the job. We need them because they are very bright and they're very eager and they're very dedicated.

I need your help. But to close with a point I've made many times: We can do this. Thanks for your time. (Applause.)

I'll take a few questions. I don't know how we want to handle them. Or are we out of time?

DALE MEYERROSE: No, we have some time. We have folks with microphones. We have time for probably two or three questions.

Q: Dr. Fingar – (inaudible). I'm curious where you see best practices either in the intelligence community or in the private sector that would aid in what you're trying to do and accomplish that you described to us today?

DR. FINGAR: I'm going to be cowardly, because I don't want to impugn anybody by referring to where I think best practices are. I think it's genuinely the case that there are good practices in many parts of the community, as indeed there are outside. But let me give some generic examples. Some of you will probably be able to figure out which components of the community do these more often than others. One is going outside, looking for expertise wherever it is found. We have portions of the community who do this routinely. They tend to be smaller components of the community because they don't have a critical mass of people inside. They have policies and rules and procedures that encourage and reward this. We have other portions of the community that recognize it as a good idea, but make it harder than it needs to be.

Look to our colleagues, our allies, and our partners for help. Information sharing with our four-eyes partners has been mentioned. They have expertise that we don't have. It is a best practice to reach out to them as appropriate. Utilizing the Internet and global capabilities, financial houses on Wall Street do risk management and make recommendations that involve billions of dollars. They're held accountable by clients. They go places and get information that we ought to tap. We need to find mechanisms to do that.

Those who have worked collaboratively – one of the observations I made after 20 years in INR was that this little organization – 160 analysts – managed to do extraordinary things to play above its size. One of the reasons was the age and experience of the analysts, which was high because the recruitment mechanism was to cherry-pick the community and bring in experienced folks. I realized it was more than just that. Because they were senior – had been around – they knew others around the community who were good, didn't care whether they were in ONI or CIA or whatever. They worked together over years. And indeed, in many cases, the people in their Rolodex were no longer doing the job on which they were expert. But they used to be really smart on Mexico, say, before they were moved to do Morocco. So they'd call them up on Mexico, and used the entire community as a resource base. And, being located in the State department, they also tapped the Foreign Service experts. So the single analyst on the country could very quickly get five or six experienced people in the intelligence community, eight or ten around the State Department, and bring their collective insight to bear on a product for which the analyst alone was responsible. It wasn't formal collaboration; it was just reaching out and asking for insight.

Now, other portions of the community do that. The sharing of information and the willingness to ask for help that is the common strand in the best practices – and there are other specific ones having to do with evaluation and product – again, CIA is a pioneer and a paragon, ahead of the rest of the community in how to evaluate tradecraft issues. They've been doing it longer and been doing it better and we don't have to reinvent it. We can start with those kinds of best practices. In a less public forum, I'd be perfectly happy to go into more detail on what I think we want to adapt out of the community or bring in from outside practice, but I am very fearful of somebody saying, ha, ha, you're taking a whack at some of our colleagues. That's not the point.

Q: I have another question and it will be brief.

DR. FINGAR: Yes, I had to find you out there.

Q: Yeah. I'm the (inaudible). It's a training and education company. My question – I want to try to keep it brief – relates to Ambassador Negroponte's letter in the national intelligence strategy document. And it talks about six intertwined characteristics, one of which is collaboration. And those characteristics are what the community currently has a vision to move towards. So collaboration is obviously something you talked about today. The other five characteristics, I'd be interested to hear what you have to say about them. They are innovation, flexibility, boldness, self-evaluative, and results-focused. So could you comment on that?

DR. FINGAR: Yeah. All of these are strands in a single rope that if we don't do all of them, we can't succeed in any of them. Unless we are self-critical, self-evaluative, unless we are flexible, adaptive, responsive, unless we are innovating in managing the flow of information or the diversity in the time urgency of the requests that we get, we'll fail. Some of these, like innovation, quite clearly are in the realm of IT, better ways of managing information; some of it – a lot of it – is in the cultural realm. "We always did it this way" is the death knell for too many good ideas. We need to move from a "why do you want to do it differently" to a "why not" approach. We ought to presume that an idea brought forward has merit until we determine that it doesn't rather than assuming that anything that differs from current practice is worse than current practice.

So all of those six elements in the DNI's letter are seen by those of us at the top trying to nudge this along, encourage, facilitate the community's thinking, are intertwined, as are the human capital, recruitment, retention, pay issues, the standards for meta-data on topics, the rationalization of who produces what on what subject in the community. We produce roughly 50,000 pieces of finished analysis a year. There can't conceivably be a market for 50,000 pieces of finished intelligence a year. There can't conceivably be 50,000 pieces of equal value. We need to go at this smartly so we can shift effort from that which is truly redundant to closing gaps, and we need to be imaginative and innovative in doing this. Flexibility invites willingness to say we tried it and it didn't work, or to try four or five different solutions simultaneously and see which ones offer advantages.

Have we moved equally far down the road on each of them? No, we're getting a little bit out of phase on these. Some are thought to be more difficult than others. But among the reasons I am so delighted to be here and thrilled by the idea of moving to the "dare to share concept" is in the innovation flexibility, and self-critical dimensions of our work. We're beginning to bump up against things that are in your world, and because they're in your world, they affect my world. And because my world isn't sufficiently innovative and imaginative to take advantage of the capabilities that you have to offer, if only we would break down the barriers, we're not where we should be. Thanks for your questions.

(Applause.)

(END)