Remarks by the Deputy Director of National Intelligence for Collection
Mrs. Mary Margaret Graham

Executive Leadership Conference
Williamsburg, Virginia

October 31, 2006

(Please click here to view the PowerPoint presentation that was associated with this speech.)

MRS. MARY MARGARET GRAHAM: Good morning. I have in the recent 18 months gotten much more comfortable speaking in public. As you might have noticed by the rather abbreviated history of my career, I grew in the operations directorate of CIA, so talking about what I did – in public – was not one of the things that I got use to. So, in the last 18 months, though, as we have stood up the Director of National Intelligence, having conversation with people like you, with the American people about what we are doing has become increasingly important. So I'm delighted to be here today.

And let me walk you through a little bit of what we are doing. And we have tried to put it in the context of what you have been doing here at the conference. You can let me know at the end whether or not we have succeeded.

Let us start with the overview of what the DNI does because there is a lot of rumor, lore, et cetera out there. The DNI serves as the President's intelligence advisor, his principal intelligence advisor. He oversees and manages the Intelligence Community – think the CEO function. And he implements the reforms that were passed under the reform act, which we fondly called the IRTPA, Intelligence Reform and Terrorism Prevention Act. As you know, in government, we always come up with an acronym to fit, and it's IRTPA.

What does the DNI not do? The DNI does not manage individual agencies. We have 16 extraordinarily competent leaders in the intelligence communities who mange the various agencies. The DNI does not execute operations. Again, the operations of the Intelligence Community are executed by the agency.

Finally, the DNI does not disrupt the chain of command. The chain of command, as you can tell, my public speaking – they are reminding me to hit my button. There we go. The chain of command resides within the individual agencies.

So let me move on to what the priorities are that we spend most of our time on. The words you see on the screen capture where we spend our time, but I think to make them real to you, let me give you some examples. In protecting the nations today, what is new? Where has the DNI made a difference?

Perhaps the biggest muscle movement, if you want to call it that of the Intelligence Community, under the reform that we are executing is the establishment of the National Security Branch

within the FBI. You have seen lots of press on that subject. But what that really means is the establishment of an intelligence discipline alongside a law enforcement discipline that the FBI is world-renowned for. That is a huge change, to build a second parallel career service internal to the FBI, which is an intelligence organization. How are we doing? It's a work in progress. But there are signs everywhere you look of the progress that is being made in developing that intelligence capability.

Another example of structures to protect the nation is the establishment of a counterproliferation center. If you think about the threats to the nation, terrorism always comes to mind first. But as close, when you think about the future, are the threats that proliferation, or WMD – whatever word you want to use – and the focus on counterproliferation in one space for the U.S. government is what the counterproliferation center is.

Making the nation safer tomorrow, that is what we are supposed to be doing. That was the demand that was laid on the shoulders of the DNI by the reform legislation. A couple of examples: We have this concept of how we should do business to integrate called mission mangers. When the DNI was asked what is the mission manager, his answer is, the mission manager does what I would do on a daily basis if I didn't have another job.

So it is focused, job one, on one mission, Admiral Redd for counterterrorism; Ambassador Brill, counterproliferation; Leslie Ireland, for Iran; Jo DeTrani for North Korea – so consistent, day-to-day, 24-seven-focus on one subject area, and drawing in all of the Intelligence Community capabilities on that particular area, building a stronger community now because we can't just take the opportunity to build something new. Yes, it's the first time that we have reorganized, restructured, reformed the nation's intelligence capabilities since 1947, but the American people, the Congress, the policymakers are very impatient, and so that – building a stronger community now is a very important focus area.

I'll give you a couple of examples. How do you build community when you have 16 agencies, some 50-, 60-more years old, each of whom has a superb expertise, each of whom has its own culture? Building community is tough, but it is in the must-do category right away. So one of the ways that we are doing that – and we have already promulgated this, and are in the implementation phase, is instilling a concept of joint duty across the community. Human nature being what it is, there has to be some keys to that to get it out the door.

And so the keys are, for those who will be promoted into the senior service in the future, in the Intelligence Community, across the 16 agencies, if they don't have joint duty in their background, they will not be promoted into the senior service. There will be some exceptions to that because you're always going to want expertise that is going to reside in one place, and live and grow in that one place, but for the most part, that building of community means that you need to understand other parts of the community as well as you understand your own.

I tell people, for example, that if I had not had the experience of spending a year-and-a-half as the exec to the Deputy Director of NSA when I was a GS-14, I probably wouldn't have the optic that allows me to continue to grow and ultimately end up in the job I'm in today. So this joint duty is very important.

Now, let me – you can see on the screen how I am going to try to talk about what we are doing in the context of what you have been doing for the last few days. All of this focusing of IT through the lens of national security is very important. So let me move right on to the first quote, that if the DNI were here, he would use himself.

The events of this summer, when we had the latest in the terrorist threat to the United States and to our infrastructure was perhaps, in my mind, and I know in the DNI's mind, the best example yet of doing what we set out to do, and that is, sharing and collaborating to protect the homeland. So let's start talking about collaboration.

Collaboration is absolutely key; it's the foundation of everything we are trying to do in building community. Increasing collaboration – I'm just going to give you a couple of quick examples. The community, as it has grown up – 16 agencies, each different, each with its own culture – believe it or not, we have never really baselined much in the community, in the days of the DCI that I grew up understand. So when we started, my counterpart for analysis, Tom Fingar, said, you know, I really don't know how many analysts there are in the Intelligence Community.

So we came up with a concept of an analytic resources catalog. Think of it right now as the Yellow Pages. Every analyst with their subject matter expertise, their phone number, their e-mail address, secure and otherwise, is in that analytic resources catalog, and there are some 18,000 of them. But for the first time, we know where they are, we know what they are doing, and we know how to find them when we need to search.

Expanded access to Intelink-U. Intelink-U is the unclassified baseline of communication within the community. If our CIO, Dale Meyerrose, were here today, he would talk to you about the three levels of collaboration, and how we not only have to move within them, but between them. The bottom level is the unclassified. And so we have succeeded by extending access to that Intelink-U by – with providing the consumers around the world a protected way to collaborate and share unclassified information from any Internet connection.

That is a huge step, because if we can do open source better than we are doing it today internal to government, my belief is we will know better where to spend our scarce clandestine or covert resource, and enabling the collaboration in the unclassified world is absolutely key to understanding and doing open source better.

The avian flu portal: another example. When we had the avian flu issue come up earlier this year, we realized that we really had no space to collaborate in, and so we built at all three levels a portal that enables collaboration across the U.S. government, whether you're in HHS, or DOD, the war fighter, the Intelligence Community, or the policy community at all three levels, and you can move among them – so one of our first successes that we can point to on collaboration.

Expansion of intelligence sharing with our allies – as you know, in Iraq and Afghanistan and many other places today, we aren't there alone; we are there with some of our closest allies, the Brits, the Canadians, the Australians, prime among them. But we have no way to collaborate; share information; open up intelligence secret and top-secret or unclassified information among

that community. And together, we in DOD, contrary to much of the press, walked down that road together, when the President said do it, walked down the road so that today the war fighters on the ground are able to share at the secret levels. And, frankly, most of the information you need to share is at the secret level.

The first-ever DOD IP cross-domain office, that is actually in your world, that is in the IT world. There is the theory behind a lot of what we are doing, contrary to much of the press, is to try to do things once for the U.S. government. And so this marriage of General Meyerrose with John Grimes, his DOD counterpart in establishment of this cross-domain management office is really key.

Sharing new tools – you can see that – it's probably – you live it on a daily basis. We are getting much more comfortable with it. The last piece is truly, for those of us that have been in the business and grown up in this business for a long time, thinking about data, not owning it, but being stewards of it is absolutely key.

All right, tomorrow, this right-to-release concept, when we're talking about analysis is absolutely key. We also have to build our intelligence support system, our IT systems so that they can share with each other to enable the collaboration that we need. Building the greater trust, that is what this whole business that we are about in this first 18 months is all about, breaking down those stovepipes pipes so when we have a problem like North Korea or fill-in-the-blank problems that – we can bring to bear the entire community instead of one agency at a time providing their expertise.

The other thing of course, human nature being what it is, rewarding the collaboration and rewarding the sharing that we're trying to inculcate in the community, collaboration in terms of a stronger community. Again, like we haven't baselined very much, lots of times our vocabularies are very different. We have got to get to the point where our vocabularies, when we use the word enterprise management or any other words that you want to use, we mean the same things across the agency.

These sound like well-yeah things, but we have never done this before, and so we have got to take the time to get our arms around this. Better sharing of the talent, I have already talked about that. The developing a common foundation, there is legacy IT across the community – sixteen agencies, 16 legacy IT systems at a minimum. There is not enough money in the U.S. Treasury to replace all of those systems, let alone the ability to step away from mission to do it.

So what we have got to come up with in this common foundation is a suite of tools that will enable us to collaborate, not an IT person. But that means to me an umbrella suite of tools that enables collaboration. But I am absolutely convinced, if I talk about collection, if I'm going to do what I want to do, create a dynamic agile collection enterprise, I can't do it if I'm not able to have the community collaborate on collection problems virtually.

So how do we share more without risking more? Most of us that are in this business as long as I have been or some of you have been know that info-tech ruled the roost for a very long time. It still does probably, but we have got to start changing our perception of risk. We have got to go

to a managing risk, whether it be in collection, or whether it be in our IT systems, or a suite of tools that allow us to collaborate. I know from my last job in counterintelligence for CIA that the tools exist today to allow us to manage the risk of collaboration, of sharing, and we just have to work not only that piece, the cultural piece of that.

For example, we have this dissemination control, which I grew up with, called ORCON, originator controlled. But do you know that today originator control is agency-specific, that sometimes when stamp ORCON on something it can't be shared internal to the community. Go back to the definition of originator control means. There was never any intent to do that. So one of things – it's because ORCON is being misused – and I can go on with other examples like that – we have got to get beyond, while still protecting the information, probably by something called role-base access, we have got to get to a collaborative way of managing risk.

The second bullet there is self-explanatory. The sharing, collaboration, freed-up tools, whatever you want to call this, has to be an organic part of what we are building. Tomorrow we are looking at new approaches for technology, but a key piece of this are the policies. If you look across the community at policies, no matter what subjects you are talking about, whether it's IT policies or human capital policies, there are policies, many of them that are 60 years old. They have become – (inaudible) – in many instances, well-meaning people, but they are (inaudible). And so the key to collaborations is as importantly in redoing the policies as it is in redoing the system.

So the policies must enable us to do the mission. The policies that the policy shop writes, whether they be IT policies or HR policies, must enable myself or Tom Fingar, collections and analysis to do mission; to the community to do its mission. And if they don't work, we should change them again, but the policy piece is very key. You see the mention there of strong identity and data management structures to enable innovation and enable collaboration. You know better than I know the tools are there for us to do that.

Risk management in the post-9/11 world, again, I have talked about most of this – new rules, new incentives, a wider perspective, a risk-management way of doing things, we do have the technology to enable ourselves to manage risk instead of just avoid it, which my belief is, is where we are walking into this change.

All right, how do we get there? This is where I diverge a little bit on the (inaudible) headline from what you have been doing. But I did because the collaborative environment is absolutely key in my mind to success; it enables everything we're trying to do.

But I did it because the collaborative environment is absolutely key, in my mind, to success. It enables everything we're trying to do. And Tom Fingar and I – Fingar and I, in talking to Dale Meyerrose, our CIO, said, "Dale, what we need is a collaborative environment to work in. And we need you, as the CIO, for the Intelligence Community to, with the community's help, build that."

I think most of what's on that slide is self-explanatory, but I'll take a minute on the last. One of the things that is a must-do, when you're trying to do something as large as reform in this

context, is there has to be constant discussion, debate, a familiar word that we've all gotten used to is socializing the concepts we're trying to work. We must do it that way because that, in and of itself, builds community. There will be times when the DNI will be directive, as he was with the joint-duty concept. But most of this is we have terrific leadership across the Intelligence Community and walking through the problems as we change gets the train moving faster from the get-go. So we do spend considerable amount of time there.

Tomorrow we're talking about system performance and that's where I go back to the suite of tools that will enable collaboration. I also think of it – again, I am not an IT expert, the way many of you are and Dale regularly pulls his hair out at the way I describe things – but to me, I'm looking for a plug-and-play. If I want to do X, we should have a suite of tools that enable us to do what we want to do in the collaboration. If I want to set up a community of interest to work the North Korean nuclear problem with all the high-level classification and the unclassified open source, I should have a plug-and-play, whether it be a policy, a process, or a tool, that I can turn to and do it quickly, not take three months to do it.

We're getting there, on that front. We had a lot of practice this summer, you may have noticed. First, we had the missile launch. Then we had the nuclear. Then we had Israel-Lebanon. Then we had Darfur, or we're living Darfur at the moment. What do we do about that? So we've had lots of practice on some of this that we're trying to build.

Now, for a stronger community, here's the customer piece. Some don't like this term "customer," but to me, it's very powerful. For the first time in my career, we have the customer, whether it be the President, the Vice-President, the Cabinet Secretary, or their deputy, setting out for us the priorities. What are the most important and what are not? And we revisit that every six months. But that's internal.

We also fully see the customer set as including people like, in the avian flu context, the Department of Health and Human Services, Secretary Leavitt. He had a need for intelligence. Just because he's not a member of the Intelligence Community, should he not be served? And the answer is, of course not. So, this in customer piece, the exercising of the "what if's." What would we do if there is a pandemic? How will the Intelligence Community respond, as a lever of government? So we get into that customer piece quite a bit and as I said, we've had some chances to practice this summer.

Now, I'm getting closer to near and dear to your heart, how do we get the tools that we need? The acquisition world – growing up in the operations business, I didn't spend a lot of time thinking about acquisition. But those of you who are with – internal to the beltway, know that when we arrived on the scene, we had a major acquisition issue to deal with called the Future Imagery Way Ahead, a program that was in extremis, I guess I would say. And we wanted to come out of that decision space, with the DNI and the Secretary of Defense on the same sheet of music. We did.

So we had a single executive branch proposal to the Hill. But, internal to that, we all got to learn a lot about acquisitions. You see the base-lining again. We'd never really done that. The acquisition policies that we're putting in place, it needs to be agile. Whether it be a huge system

or a small system, we can't roll them from year to year to year to year in the 10- and 15-year range. There will exceptions to that, I'm not making a blanket statement, but acquisition needing to be more agile to respond to agile mission demands, is absolutely key.

Here's the tough one. Transforming the acquisitions mentality. The policies, agile. Actions based on genuine needs. I'm sure I don't surprise many of you when I tell you, that my opinion is, the requirements system is broken. The Intelligence Community adds on requirements as if they were sprinkles on a candy cone – (laughter). And part of the problem of acquisition that we're in is because we are not rigorous in stating our requirements and sticking to them. So we've got to get better.

The next one: balancing what we want with what we have. I've been spending a lot of time the last 10 months, developing the first piece of an integrated collection architecture. What capabilities do we need, as an Intelligence Community, in the future? We don't have anything like that. But, we're coming out the end here on the technical side of that. We'll add the rest of it in the years to come. The first thing we did is, what do we have in the current – (inaudible). What's our program of record? And the next question, what are the shortfalls, based on the capabilities we say we need? And then, we've got to fold in our acquisition process based on what we need and try to be rigorous in that.

The budget that we will operate on, yes, it is huge. I would not disagree with you. But in its own way, it is finite. We had a big bump in the intelligence budget because of 9-11. But as far out as I can see, I think it's going to be fairly flat, so all the more reason to do acquisitions carefully and correctly. Dale Meyerrose, actually, as our CIO, has a very interesting view on this, which I subscribe to. When he talks about building a suite of tools that we need to enable collaboration, he doesn't think in big acquisition terms. He thinks in, "think big, start small, and scale fast." It's an entirely different way, I think, of thinking about how we do acquisitions.

Effective acquisition in the Intelligence Community, we're working on it. Again, you're seeing the collective here. Not the individual agency. The acquisition policies that we're going to put in place will be community policies. Yes, there'll be tweaks on individual agencies that will be necessary, but basically, the excellence we're looking for is community excellence.

So, I've come to the end of my prepared remarks and slides. I don't think I did too much damage to the slide presentation. I covered what I think, if the DNI were here, he would want you to hear from us. What are we doing? Are we serious about it? And that to enable what we're doing, building communities, making the nation safer today and tomorrow, we believe collaboration is the enabler that is going to allow us to do this. So with that, summing up, I will open myself to questions, which I will try to answer. If I can't, we will get you an answer. We've got about 15 minutes before we have to hop back on the plane and head back for the rest of the day in Washington. So with that, I'll open up to the floor.

Q: (Inaudible.)

MRS. GRAHAM: Well, one thing that I did not mention that I think will be familiar to all of you, there's this acronym called TPED [Tasking, Processing, Exploitation, Dissemination],

which is all about processing, exploitation, and dissemination. We could collect all we want, but if we don't have the processing, exploitation, and dissemination team right – integrated, we are not going to succeed because the magic in a lot of the intelligence systems is on the ground. Whether it be a technical collection, whether it be a human collection, the processing, exploitation, and dissemination is enabled by IT.

And we've got to – we've always, I'm told by people that have been at this collection business much longer and in a broader sense, in this broad sense, than I have – we have always shortchanged the ground processing, exploitation, and dissemination. We have to stop doing that. Interestingly enough, in this first year do-out, from the integrated collection and architecture that the community is doing under our guidance, to inform how we spend the '08 budget billed, there is a significant piece of ground there. Interestingly enough, not enough. So, as we go into the second year, we're going to spend a lot of attention on that because why would we build these multi-billion dollar – whether it be a human being trained or a technical means to collect if we're not using the information correctly because we haven't processed it or exploited it or disseminated it correctly.

Others?

Q: (Inaudible.)

MRS. GRAHAM: Let me take the back end of that question first. The incentives are built in somewhat in the human-capital process. Not to the degree that we would like yet. But let me take the back end – because all the work we're doing, we cannot forget, if you think of what we're doing as a train with the customer piece at the front, the caboose of the train that we've never been terribly good at is evaluation on how we're doing. It is absolutely key in the environment that we live in, whether it be the budget environment or the environment that is the American people's expectations of us, demands of us, or the policymaker's expectations and demands, that we do evaluations. How are we doing?

We've set up some of that, and the best example I can give you – after we had our first opportunity to practice what we put in place earlier this summer with the aborted North Korean missile launch, Tom Fingar and I said, you know, we really ought to take a minute and step back. And so, we actually did – whether you call it a lessons learned or an after-action review, in about a two-week period. Interestingly enough, by – we didn't do it ourselves, we had another piece of the ODNI, who wasn't quite so engaged in the process of collection and analysis, do it for us. And the answers out of that, we were able to do a quick turn on some of them – not all, but some of them, and we're already seeing the benefit of that in the North Korean missile exercise.

The incentives to collaboration, I would say, if I were grading us, I would say we're probably at a B, getting the right incentives in place. But it's interesting, every time you have a success at collaborating on a piece of a problem, it engenders more willingness to collaborate. People say, oh, that really worked. And so, the next time you're bringing them back to the table, they're more willing to come back to the table.

Others? One more. One last one.

Q: (Inaudible.)

MRS. GRAHAM: In fairness, I will tell you it has nothing to do with the energy of our CIO. What it has more to do with, in my own mind, goes back to the issue of, this is the first time that we have truly tried to do this, since 1947. And so, as we began to build and we could put checkmarks against some of the to-dos, the richness of the experience began to leave, particularly, Tom Fingar and myself, the DNI, the Principal Deputy, toward, we have got to have a collaborative environment. So, I would say our discussions with the CIO saying, Dale, we need to do this more and faster than we have been.

Some of the examples I gave you are examples of how we've done things, like the sharing with our allies, like the portal we've did on avian flu, those were point solutions. And what, about four months ago, we got to the point where, we have enough examples of success and enough people saying, you know, you do a lot better if – across the community; that it really crystallized for both of us. So I would say that train is gathering steam and the collaboration environment is getting larger by the day. I am a glass half-full person; I'm convinced you need that in an effort like this. But I will tell you that there are examples of success; and I will also tell you that there are plenty of inhibitors still out there and you just have to play Whack-a-Mole one at a time – (laughter).

Thank you all very much.