Remarks and Q&A by the Director of National Intelligence
Mr. Mike McConnell

ODNI Open Source Conference
Washington, DC

July 17, 2007

MRS. MARY MARGARET GRAHAM: Good morning, everybody. I'm here to introduce somebody who I don't think needs any introduction, but as you know, the Director of National Intelligence, Mike McConnell, was sworn in as the nation's second Director of National Intelligence on February 13th, 2007. Director McConnell has a rich history has a rich history in the intelligence community, and is truly what you would call, in our own vernacular, an intelligence professional.

I had the great pleasure -- although I don't think any of us predicted that we'd be where we are today -- of working for Director McConnell when he was DIRNSA (Director of the National Security Agency). I got kicked out of the nest that I grew up in at CIA and sent, of all places, to NSA as an executive assistant, and so I had that opportunity a lot of years ago when I was a lot younger and a lot taller – (laughter).

So without any further ado, and without going through his bio for you, which I'm sure you all know, I'd like to take the opportunity to introduce you to the Director of National Intelligence. It's our pleasure to have him with us today, and I think he's looking forward to talking to you about something that's not classified. (Applause.)

MR. MIKE McCONNELL: Thank you very, very much. What Mary Margaret left out was she was 6'8" when she started that job. (Laughter.)

I generally prepare speeches en route from wherever I am to wherever I'm speaking. The ride was from the White House to here, so this is going to be from the heart. I'm going to speak to you about a number of things. There was a prepared remarks, but I generally prefer not to read to you. I'd rather – I've got something to say – if you want to read it, I can hand it out, but let me talk to you a little bit. I'm going to do three things: I'm going to give you an overview of what I'm attempting to do in this community to get us prepared for current threats and future threats, and it's a big change. Many of us, particularly Mary Margaret and I, grew up in a Cold War mentality, and we have changed and we are changing, but we must change even more. So I'm going to give you a little overview of that.

I'm going to tell you one quick story and a couple of comments about what this conference is all about, and then I'm going to talk to you about current threat. What is being released today is an unclassified version of the key judgments for the current threat and terrorism to the United States homeland. And so I thought I would provide some of that background, and then hopefully we'll have some questions, an opportunity for a little dialogue at the end.

Let me start with just an overview of the community -- how do I think about it and what it is I'm trying to do. And when I say community, of course I'm talking about the United States intelligence community, which is an extended community because we have relationships and partnerships with many other nations.

The first word I would use is a much higher level of collaboration. When Mike McConnell comes and goes, as we all do in these jobs, if there's a bumper sticker and there's one word to describe him and my time in the community, I hope it says "collaboration," or at least "a better level of collaboration."

I think all boats rise. We achieve significantly more when we work together, and that's true in anything from an athletic team – little league to professional – to a business to units of government, and it's particularly true across a community that's as wide and disparate as the United States intelligence community.

There are 16 agencies; most of those intelligence organizations, a vast majority – 15 of the 16 – work for another cabinet officer. So the founding legislation in the Intelligence Reform Act and Terrorism Prevention gave us a framework, but it didn't quite capture what the authorities needed to bring the community together in a way that was compelling, and I would compare it to legislation in the late '80s that governed how the U.S. Defense Department operates. That legislation is known as Goldwater-Nichols and it created and actually forced a level of jointness. Everybody was opposed to it early when the deliberation was taking place. It took six years. Within one cycle of Joint Chiefs after the legislation was passed and a higher level of collaboration and jointness was achieved in the military, the Service Chiefs all testified: greatest thing that ever happened to the United States military.

So that's kind of the framework about how I think about this community and what it is I'm trying to accomplish. I want to integrate the community and achieve a much higher level of information sharing. Now when you say information sharing to an intelligence professional alarm bells go off, and the reason is we also have another obligation called protecting sources and methods. And so if you're sharing information, there's always risk to compromising a source or a method, and at one level if you compromise a source, you might lose the source because the way you're getting information would be changed. At another level, if you compromise a source, you might cause someone their lives.

So this is a very serious business, and while I am pushing collaboration and information sharing, what I hope to do is to create tension in the system so that analysts think in terms of a responsibility to serve a set of customers, and they're pushing to provide information to those customers wherever they may be – White House, military, down to the foxhole, across to a governor, over to a mayor, over to a police chief. Wherever that information is needed, we need to think in terms of responsibility to provide it.

The other flipside of that coin is we have to protect sources and methods, so there's tension, and appropriately so. The tension needs to be there – very similar to the U.S. Constitution. If you think about the origin of the Constitution – freedom and security – good words, but it creates tension between the two paradigms. So that's the way we're trying to think our way through it.

I want to transform analysis – not me, personally, but to have the system transform analysis -- much more rigor, challenging assumptions, challenging key facts, highlighting dissent, creating it in a way so that you do alternative analysis, red teams, to ensure that the final products that we turn out are the best possible products for our major customers and, of course, for the nation.

We have a system of security procedures that were established, quite frankly, in World War II, and they've served us well. They served us well in World War II, they served us well in the Cold War. My hypothesis is they do not serve us well today. We have to go faster, we have to reduce the bureaucratic burden, and we have to have a better level of monitoring.

Where does this model exist today? It exists in the financial community. The financial community can clear members of their organization to process billions of dollars in transactions for which, if they could slow the transaction for a second or two, one could engage in arbitrage and make millions of dollars personally. So if you can clear people to handle those volumes of money or that kind of incentive, and you can do it in something like two weeks, why does it take us six months to a year, in some cases even longer?

So we want to change that, but now what's the difference? All the spies who came into our system years ago for the most part were incentivized by money, and for the most part, they didn't know they were spies when they came through. Once in and they turned out to be a spy, then they knew how to beat the system from the inside. How does the financial services community deal with that? Keystroke monitoring. It doesn't mean every keystroke is monitored, but it means it is monitorable. So if we set up lifecycle observations among those who choose to serve and we go faster, we can bring them in sooner, address more current problems – language, cultural understandings, open source information, the kind of information that this conference is focused on, but we have a lifecycle monitoring process that, at least in the model used in industry, is more effective and is cheaper.

One of the biggest challenges that we have is to integrate foreign and domestic intelligence. We know how to do foreign intelligence. That's what this community was founded upon. We're approaching -- and later this month, the 26th of July will be the 60th anniversary of the National Security Act in 1947. That act founded the CIA and the Director of Central Intelligence which has now morphed into the position I currently hold, the Director of National Intelligence, attempting to coordinate across all those 16 agencies.

Foreign intelligence was very focused on the Cold War. It was quite effective. It's the world I grew up in, the world that I knew, and had great confidence that we could serve the nation's interest. 9/11, when terrorists left foreign soil, crossed here to the United States and carried out that terrible act on the 11th of September, they were foreigners, but they were, in the U.S. context now, a U.S. person. They're on U.S. soil. It's a domestic problem. So that interface between foreign and domestic is something we have to spend a lot of time on to ensure that we have the appropriate laws, the appropriate authorities, the appropriate process. We know how to do criminal investigations; we've been doing that forever. We know how to do foreign intelligence. It's this foreign and domestic integration intelligence which is a key that we need to spend some time and effort on.

Another area is acquisition excellence. We've had the ability, with special authorities in this community, to go fast, spend large sums of money to solve major national problems. That's gotten away from us in the past 10 or 15 years. It's become a little more bureaucratized, a little more formal, a little more processed, and – (inaudible) – it takes one and a half to three times the money, and as much as three times the time, to build a major capability. So we want to go back to the way it was in the '60s, '70s and the '80s – when we tended to have a major problem, we would risk failure to solve that problem, and we would spend large sums of money, often, to invent new technology. And we want to try to recapture that. I won't go into a lot of the details about why we lost it or what the background is unless there's a question from the audience later on.

One of the things that we have to focus on is world-class expertise in language. Those who threaten us today come from very diverse groups, very diverse backgrounds, and our level of expertise with language and understanding tribal customs and cultural issues and so on needs to be improved, and one of the ways we're going to try to do that is to recruit into our community more first-generation Americans so they can help us work these very difficult problems.

We're going to attempt to modernize our business practices so we have audit records that stand and are reliable and the process more appropriately captures the process in industry for running a business. This is a large business. The top number is classified. A lot of you all guess at what it is. I won't comment on your guesses, but it's a large sum and it needs to be more appropriately monitored and audited in a way that meets commercial standards. And sort of the bottom line, from my point of view, is a more open and candid dialogue, not only with our customers, but with the Hill and certainly with the American public, and that's what I'm going to comment on here in a moment when I get to my comments about the current threat.

I'm sure you've heard this in the course of this conference: open source – less than a hundred terabits in the Library of Congress – that's a huge number – but over 600,000 terabits moving through the internet today. So the challenge for my community becomes 99. – you name it – 9, 0.8, some huge number of all that 600,000 terabits moving through the internet per year is all unclassified. It's all open source.

So what’s our challenge? Our challenge is to have it available, to sort it out, to be able to touch it, to be able to examine it, to be able to have it useful in the context of the problems we’re attempting to work.

Now the flipside of it is – you pick the number, 0.01, 0.02, 0.09, whatever, it’s some number – is classified. It’s secret. It means it’s something that somebody wants to deny the United States from knowing for whatever reason. It’s a weapons system, it’s a terrorist plot, it’s a strategic war plan of some country, it’s a political dialogue inside a country, it’s a diplomatic strategy. That’s the kind of information that our community has asked to obtain and to analyze and to integrate and to understand and present it to our senior decision makers. So the targets that we worked – targets in the sense of foreign targets we try to penetrate and understand – our job is to penetrate, collect information and understand. We do that a variety of ways. We can take pictures, we can listen to their communications, we can recruit sources, we can have special sensors, but it’s all an effort to capture and obtain information that somebody wants to deny this community and to this country. So the challenge becomes are we effective in getting that information, whether it’s a battlefield situation or strategic planning or a long-range threat, and then combine it with open source and combine it in a way that’s effective.

One quick story: I got to serve years ago – it seems like forever, but years and years ago, I reported to the Joint Staff – the Joint Staff in the Pentagon, Joint Chiefs of Staff, as a new intel officer for the chairman, General Powell. I reported for duty – ready to take my job, sir – and five days later, the Iraqis invaded Kuwait. I remember very clearly – I am of the naval service, maritime service as we say, a sailor, and I had on white shoes, white trousers and a white shirt, little shoulder boards – I looked pretty spiffy in my uniform.

Sailors don’t know a lot about ground warfare – (laughter) – and the guy that I was talking to was General Colin Powell who was a ground officer. So it was going to be an early challenge. The other customer – major customer – was General Schwarzkopf who took no prisoners as he did his war planning, particularly if a sailor was trying to explain something to him. In his vernacular, I was a squid – (laughter) – but the effort was to learn a lot quickly and to move fast.

Well, early on, one of the questions that came out is if we move tanks into Kuwait and into Southern Iraq, what’s the condition of the soil, and will they sustain tank movements or armored personnel carrier movements or major equipment. I remember when that movement occurred; it was the largest concentration of fighting power in the history of the globe: two major armored divisions moving from Saudi Arabia into Kuwait in the southern part of Iraq.

Well, you could get the information you needed if you sent a team, but that’s risk and also could compromise what you’re trying to do. So we did open source. What we found was something that was not only open source, it was 100 years old. A team riding camels went through that area 100 years ago on an archeological expedition, but they were methodical about capturing soil conditions and recording them, and guess what –

the soil conditions didn't change in 100 years. So we found that information buried in some library somewhere very useful in doing some of our initial planning so we could understand the conditions of the soil.

Now, I'm sure there are many, many stories, and I'm sure you'll hear a number of them today. Part of the challenge we have, we the intelligence community have as we embrace open source, the 99.X percent that's unclassified, is first, we've got to know how to do it. There's some special training about understanding it, how to access it and so on. And then, how do you add value? We live in a classified world, no windows, secured vault, secrets, top-secret, confidential, that's the world we live in. How do you take this broad, vast, unclassified world and then add significant value? I think that's our challenge.

We've always had access to open source. We've always listened to the broadcasts that come from around the world. But I think there's a value added that we're still searching in a way that causes the entire community, not just the Open Source Center, not just the ones that used to operate the Foreign Broadcast Information System, but all analysts.

The other thing that's missing are the tools. Currently our systems are, for the most part, closed. It's difficult for some of our analysts to have access to the web because if you have access to the web, now there's a challenge that, well, I'm working in a classified environment – what happens if I cross connect and do I compromise and do I cause some of my secrets to slip away? So having robustness in our knowledge, our ability to think through the value added, and our ability to have the tools that are world-class – and most of those tools are built here in the United States, so we should be able to capitalize on that.

Let me turn now to the terrorist threat against the United States homeland. This was produced by the National Intelligence Council, nickname was the NIC or the acronym is NIC. The 16 agencies of the community coordinate on all national intelligence estimates. I get to chair the final review, where we can hear all players if there is a dissent or a problem or an issue – do we need to send it back? Is there something we need to resolve? – and so this particular assessment has been in the works for a long, long time. All these issues have been debated and reviewed and worked off and so on.

It's a classified assessment. It's classified at the top-secret level, top-secret level. What we were asked to do is to look at a series of the key judgments and make them unclassified so that we could share them more broadly and in particular with the United States public. And I'm going to run through some of these key judgments and then I'll save some time and the end for some questions.

The first and foremost of the national intelligence estimate on the terrorist threat to the United States homeland is that there is and there will be persistent and evolving terrorist threats over the next three years. The time period for the assessment is three years out. The main threat comes from al Qaeda. This is al Qaeda, Osama bin Laden, Zawahiri, currently operating in the federally administrated tribal areas, the frontier area of northwest Pakistan on the border with Afghanistan. This threat is driven by undiminished intent – undiminished intent – to attack the United States homeland. These groups have continued to adapt and to improve their capabilities.

Now, the first question that usually is asked: well, wait a minute, are you saying that al Qaeda today is as capable as it was in 2001? In my considered judgment, the answer is no, they are not as capable. They were close to being destroyed when the United States and our allies invaded Afghanistan and attacked the Taliban and al Qaeda in 2001 and carried out through 2002. Some of the leadership escaped to the border area and into Pakistan, where they're currently enjoying sanctuary, and they have attempted to rebuild. It's significant rebuilding, but are they as capable as 2001? I don't think so. Some could take a different point of view and may argue it, but in my judgment, looking at all the data, they are capable, they are planning, but they are not as resilient or as robust or as capable as they were in 2001.

The efforts that the United States has led, both with our allies and then actions we've taken here in this country, have greatly increased and our greatly increased worldwide counter-terrorism efforts have constrained al Qaeda and their ability to attack in the homeland. Al Qaeda Iraq – there is an al Qaeda Iraq; it is a direct affiliate of al Qaeda leadership, which is Pakistan – is carrying out terrorist attacks on a regular basis, suicide bombings, roadside bombings of convoys and so on. But al Qaeda the larger has been constrained in its ability to attack the United States because of the actions that we've been taking.

This had led terrorist groups – and there are a wide variety of terrorist groups; al Qaeda is extending its reach to try to incorporate with more terrorist groups – but it's led most of them to perceive the U.S. homeland as a very difficult target to attack. The direct disruptive measures have disrupted known plots since 9/11, relatively large number of plots that we've been able to thwart since 9/11 because of these efforts to target and penetrate and understand and disrupt.

Our concern in this assessment, looking out three years, is that the level of international cooperation may wane as 9/11 becomes a more distant memory and perceptions of the threat decline. That said, al Qaeda is and will remain the most serious terrorist threat to the U.S. homeland. Its central leadership has stated its intent and continues to plan high-impact attacks. That's going on today. It was going on last week, it was going on last month, it was going on last year.

Al Qaeda is pushing other extremist groups to adopt its efforts, to swear allegiance and to supplement al Qaeda's capabilities. Now, here's a way to think about al Qaeda 2001 and al Qaeda today. They've regenerated key elements. I've spoken to some of them, but let me give you the list, a list of four. The first is they have sustained the top two leaders, Osama bin Laden and Zawahiri. The second is they've been able to recruit and mature new lieutenants to lead the fight, to manage the operations, to manage the money, to plan the operations, to oversee the movement of forces and so on. So they have the top lieutenants to train and control operations.

Third, they are enjoying a safe haven or sanctuary in Pakistan. We are working very closely with the Pakistani government. President Musharraf is moving forces, again, into that region to put pressure on al Qaeda and the Taliban, who are in that northwestern segment of his country. In the past few days, the Pakistani military has lost over 80 of its soldiers in an attempt to put pressure in that area. Those are the first three. The fourth one, how would they be successful here in the United States, is proving a little more difficult for the reasons I've indicated. We've gone to great lengths to target them, to disrupt them and to make it difficult to get into the country.

The fourth thing they're working as hard as they can is positioning trained operatives here in the United States, and as I've said, they're working very hard to overcome that. They have recruitment programs to bring recruits into that region of Pakistan, particularly those that speak the right language, that have the right skills, that have the right base that they could come to the United States, fit into the population, and then use some of the training that they receive in the Pakistani area for explosives and so on to carry out acts, sometimes recruiting other cells. The intent, clearly stated, is mass casualties – mass casualties larger than 9/11. Their intent is mass casualties, and their intent is spectacular destruction -- spectacular destruction, something like a building falling or something.

We are, here in the United States, in a heightened threat environment, and that's going to continue for the foreseeable future. Al Qaeda will try to enhance its capabilities to attack the homeland through greater cooperation with regional terrorist groups. I mentioned al Qaeda and Iraq earlier. They are engaged day to day. They're battle-hardened. They have lots of experience. They know how to build explosives that can be incredibly destructive. And al Qaeda in Iraq helps al Qaeda leadership in Pakistan energize a broader extremist community, raise resources, recruit and indoctrinate operatives. Al Qaeda's homeland plotting is focused on political, economic and infrastructure targets. I mentioned mass casualties and the visual dynamics of major destruction.

Another area that we focused on that we're very worried about is the al Qaeda leadership has now tasked its operatives to acquire and employ chemical, biological, radiological and nuclear material -- chemical, biological, radiological and nuclear. Radiological, nuclear, why would there be a difference? You could take something that's radioactive and just cause an explosion, just spread it around and have contamination. If you pursue nuclear in a different context, you could describe it as nuclear yield. So we know they are attempting to obtain these materials.

Another group that is of concern is the Lebanese Hezbollah. Hezbollah has not attacked the United States interests directly, of course, here in the United States, but we worry about sleeper cells here in the United States, and if we cross some Hezbollah red line, they feel threatened by the United States, we feel confident that they would task the Hezbollah operatives that are here to engage in terrorist activity.

One of the things that worries us the most are the Internet websites, open source. This conference is focused on open source. I would ask you just to take a look at some of these websites. Radical and violent extremist training, and the websites are expanding in the West, both in Europe and here in the United States. In addition, the globalization trends, the technology advances, what we're talking about in this conference with regard to open source – allows these people to find each other. Not only do they justify some of their thinking, but it actually can intensify their anger and mobilize them to attack. And all that happens without requiring any centralized leadership. The centralized leader can provide philosophy and oversight and guidance and justification, but not necessarily control each individual act.

Our ability to detect broader and more diverse terrorist plotting will be a challenge for us in the years going forward. We achieved a fairly significant level of capability. The terrorist groups have suffered as a result of our ability. They are adjusting their thinking and their tactics and their process. And they are attempting to find sanctuary that would allow them to continue to rebuild and to infiltrate the operatives.

We are attempting to improve our capabilities, update our laws, and our authorities for appropriate surveillance. And we have to do that, of course, consistent with observing the terrorists – foreigners – while protecting the civil liberties and the privacy of Americans. And this community is working very closely with the Department of Homeland Security and, of course, the FBI, the Congress, and others in the administration to do whatever is needed to prevent these heinous acts from being carried out.

I think what that, we have a little time left. I'll stop and see if we can't take some questions.

(Applause.)

Q: David Kamien, CEO of Mind Alliance Systems. Sir, what steps are you taking to be able to manage the flow of communication and information so that you can improve it over time? If we took the 9/11 plot exactly as it unfolded and we mapped the flow of communication from intercepts as a trigger all the way through response, do you think we would be able to hold our heads up high and say the flow of communication for that very same scenario is where we want it to be today?

MR. MCCONNELL: One of the things that we're doing currently is working with the Congress to update legislation that was enacted back in the late '70s. It's referred to as FISA, Foreign Intelligence Surveillance Act. When that act was passed, it set up a condition differentiating between wireless and wire. And it was passed for good reasons; it was passed because there were some abuses by this community internally –

want to prevent those in the future. But it was passed also recognizing the need to do foreign intelligence collection.

Well, because of the words in the bill in the late ‘70s, it was captured in a way that when technology shifted, wireless less so in the international context and wire more so, it handcuffed us. So it put us in a situation where now today we are required, in many cases, to secure a warrant to do foreign intelligence collection, foreign surveillance. So we are working with the Hill – I’ve had a chance to meet with a large number of senators and congressmen – to explain the backdrop and why this is an issue. And I think we’re on a path to get that corrected. If we do get that corrected, we would return to a level of capability that you are describing that was inhibited somewhat in the 9/11 timeframe.

Q: Sir, Dave Ribabi (sp), Apogen Technologies. Sir, you have at your disposal the greatest intelligence community on the globe. What do you find to be your greatest challenges today in tracking down our nation’s enemies and locating them, identifying them, and destroying them?

MR. MCCONNELL: That is not an open source answer. (Laughter.) No, in all seriousness, we do have the greatest intelligence community on the globe. And it’s being very effective. The kinds of things that I outlined early – my early part of my remarks – if we can come together in a tighter sense of community, I think the performance of the community would be substantially enhanced.

Now, what do I mean by that? In this town, you frequently hear a word, stovepipe. And depending on who you are or what your intent is, most of the time, if you say stovepipe, that’s a perjorative; that’s an evil term, because the mindset is you have some discipline – signals intelligence or human intelligence or imagery or geospatial, whatever it is. And you live in your stovepipe and you control information and you don’t share it.

Well, let me go on record to say stovepipe is a good thing. And the reason I think stovepipe is a good thing is because it gets you technical depth, excellence, people who spend their careers in a discipline that you could never get to that level without some specialization. So think of specialization, compare it to brain surgery. You wouldn’t want to go to the local auto mechanic for brain surgery; you’d want someone who had spent a lot of time doing brain surgery.

So while our stovepipes are wonderful things, the challenge for us is now to connect information across the stovepipes. So my biggest challenge as the new director of National Intelligence is how do you get this level of collaboration and coordination and sharing and trust when you have to move information outside the stovepipe.

The way I think about it – this is actually the world I came from as a youngster growing up – is the all source environment. If you’re going to address a problem for a military commander, the president, national intelligence estimate, whatever it is, you have to have all sources of information. And that means that sometimes the technical parameters of something that somebody in a specialization would want to protect for security reasons. So that’s the challenge.

I would say a second part of that is achieving collaboration in the sense of jointness the way the U.S. military has achieved jointness. When we have a situation using military force today, the chain of command is very short – the president, the secretary of Defense, the area commander, and the joint taskforce commander. And the joint taskforce commander is someone who has command of Army, Navy, Air Force, Marine forces, whatever the task is. So that level of jointness has caused the U.S. military to significantly increase its capabilities. I think this community can do the same thing if we have a similar approach. And we’re going down that path.

Q: Gordon Middleton, Patrick Henry College. Sir, I’ve had the opportunity in another context to hear you share about some of your previous experience in private industry in some of the approaches that were effective in accomplishing – if you will – organizational and substantial cultural change within that context that you’re looking to perhaps use some of those same things in the intelligence community.

One of those things that you’ve talked about is your use of the ExCom, with bringing together some of the senior leaders in the agencies. Can you share with us any things that are ongoing in that context, specifically in the context of open source, and how those two things may be coming together and how you might be using the ExCom to push some of the open source initiatives?

MR. MCCONNELL: Thank you, very good question. When I came back to the community, one of the things that I left the community – some years ago, 10, almost 11 – is there was to me it seemed like some unfinished business. I made my case, but I was never convincing. And what I was trying to make my case back in those days was for the director of Central Intelligence to be more inclusive in bringing the agencies into the fold to work issues.

And so, what I decided to do when I came back was to establish an executive committee. And the thinking on the executive committee is, if you’re a major organization in the community spending billions of dollars or if you’re a major consumer – State Department, Defense Department, Department of Treasury, so on – you should be at the table.

And the thinking on my part was to organize it a little bit like some industry players. Many industries have a very small, lean corporate headquarters, and they have lines of business – some would even say separate businesses. But when they need to make corporate decisions, they come together as a unit. You put the tough, gnarly, unpleasant problem on the table, and the deal is, we don’t leave until we get this resolved. Now, reserving 51 percent of the vote helps a little bit. But we’re working through those issues.

I've mentioned collaboration and how we're trying to get there. One of the ideas is a 360-degree appraisal. That's very different for this community. Normally, you've got a boss; the boss writes your appraisal. All of them are inflated. I grew up in the system. I tried to change it for years. In my system in the Navy years ago, if you weren't 1 percent – meaning you were ranked in the 1 percent category – you would fail to be promoted your next promotion. Well, that's ludicrous, because everything's a bell curve.

So what I wanted to do was to say, let's make it meaningful. And in my experience in industry, one, in the company I was in, we did it to ourselves and it worked out so well, we sold this to others who were trying to do a similar thing.

What is a 360? Seniors, peers, which turned out to be most important, subordinates, clients – seniors, peers, subordinates, clients. And the appraisal is not written by your boss or anybody in your chain of command; it's written by someone who knows the community, knows the issues, but writes the appraisal and the context is developmental. Hey, you're really good. We really appreciate what you're doing. But what is it you could do to make yourself even more effective, to make the organization more effective?

Now, as you might suspect, a little hesitation and resistance. Well, wait a minute, I've never had an appraisal like that. And I'm not sure how I might react to that. I must add, the first one I received in industry compared to the ones I had on active duty, I thought, oh, this is not going to work. (Laughter.) But I have to say, after a couple years, I learned the value of it. It let me then – it enabled me – it allowed me to focus on specifically what I could do to be more effective in my business world.

So I think if we can embrace this – and we're going to try – I volunteered to be the first one. We've gotten someone from senior from the Department of Defense. The people that they will start with are my ExCom, the deputy directors in ODNI, and then I told them go wherever you want to – Congress, the White House, major state, major customers.

And what I'm asking for us, you've seen the plan. We had a 100-day plan. We're drafting a 500-day plan. We're trying to set up a set of deliverables so we've got something to work against and we can hold people accountable. So if there's some part of this that I'm doing wrong, Mr. President or Madame Secretary or Mr. Secretary or Congressman or Senator, give us some input here to help us get a course correction.

So I think if we can embrace that, and we work this ExCom, and we try to work as a community, I think we'll achieve a higher level of effectiveness because it will be tighter integration.

Q: Mr. Director, it's Lou Martinez with ABC News. Can I ask you which is going to be a greater factor in the continued growth of Al Qaeda, Al Qaeda in Iraq – the continued growth of Al Qaeda in Iraq – or the continuance of a safe haven in the tribal areas? And also, can I ask you, is there preliminary assessment by the intelligence community as to what would happen in Iraq should the United States pull out?

And a third question – (off mike) – Sudan, the United States intelligence community's relationship with Sudan, has that borne fruit? Is that a beneficial relationship between the United States and Sudanese intelligence?

MR. MCCONNELL: I'm going to take a bye on the last one. You don't get three questions; that's not fair. (Laughter.) And I'm going to combine the first two, so you're down to one question. (Laughter.) Iraq and Pakistan, both are growing, are becoming more capable.

The differences in Pakistan, they have the inspirational leadership, those who justify these heinous acts, and they have sanctuary. Now, we're doing everything we can to disrupt that sanctuary, as is the Pakistani government, as are our forces who are located just across the border.

In Iraq, currently, in some areas, we have Al Qaeda in Iraq on its heels. And the reason for that is the Sunni population in which they are operating have turned against them. Now, you may recall, if you've worked this particular problem and focuses on it, there is a problem out to the West called Anbar. Anbar province clearly was stated, the Al Qaeda in Iraq, that was their center of operations. They were going to control it; it would be their sanctuary; it would be how they would do their plotting, and then go into Baghdad and so on.

Because of their tactics, because of their engagement, the way they carried out such terrible acts – demanding, forcing, killing children in front of their parents, that sort of thing – the local sheiks in that region, the tribal leaders, said enough. And so we worked with them and they worked with us; and that started to change. So Al Qaeda is certainly in Iraq; it's not defeated. But it's back on its heels a bit.

Now, that stated, the political dimension, we have a debate in this country about what to do going forward. We have some benchmarks that we are trying to get achieved between now and September. The stated intent of Al Qaeda in Iraq is to raise a level of violence, suicide bombing, and roadside bombings to the highest possible level for maximum loss of life, and major sustained destruction. That's their stated intent.

So what we have going on is we're being effective in some dimensions about turning it around. A level of security has been improved in some areas. The jury is still out about how it's going to be effective in the long term. But those in Iraq read the newspapers. They are very conscious of what is said in the U.S. public and the U.S. news media, and they know what the debate on the Hill is. They know what's going on. So if they can raise a level of violence for a short period of time, they believe they'll achieve their objectives.

So now it’s a long answer to your question. Pakistan sanctuary is a major issue. In Iraq, they have attracted foreign fighters; they have recruited Iraqis. It’d be interesting for you to know, I’m sure, that most of the suicide bombers of Al Qaeda in Iraq are not Iraqis. They come from the outside.

I am getting the hook. (Laughter.)

MRS. GRAHAM: You know, there is an old maxim that it’s never a good idea to surprise the boss. But one of the things we wanted to do to thank him for his support to this conference that we are doing as the inaugural DNI Open Source Conference was to bring some coals to Newcastle. So we have a little box here that we’re going to give him that has one of his very own coins in it. (Laughter.) But on the top of it is the DNI Open Source Inaugural Conference. So we wanted to thank you; we wanted you to notice what was behind you.

MR. MCCONNELL: Oh, my goodness.

MRS. GRAHAM: Some of us aren’t used to speaking in public and seeing our faces the size that these screens are. But thank you very much.

(Applause.)