



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

John F. Kennedy Jr. Forum at Harvard University

**Harvard's Kennedy School of Government
Cambridge, Massachusetts**

December 2, 2008

MR. TONY SAICH (Director, Ash Institute): Good evening, everybody. It's a great pleasure to be here this evening for what I'm sure is going to be an interesting program. And we have with us tonight one of the nation's leading national security experts who not only serves this country as the second Director of National Intelligence, but for us at the Ash Institute and at the Kennedy School has a special relationship and significance for us, and that is that our speaker tonight was selected from a pool of something like 1,000 applicants as one of only six recipients of our 2008 Innovations in American Government Award. And that was presented at a beautiful ceremony we had in Washington a little bit earlier this year. And it's a prize which is given annually to initiatives within governments at different levels that exemplify excellence in creativity in the public sector.

So this year's winning initiative from the Office of the Director of National Intelligence was designed to address unique threats faced by American Intelligence Community as detailed in the 2004 Intelligence Reform And Terrorism Prevention Act and the 9/11 Commission. The program instills a new model of collaboration by requiring personnel to serve a period of duty outside of their parent agency as a prerequisite for senior level promotion, so an effective way of trying to integrate different elements of the community. As a result what is referred to as these joint duty personnel gain a much deeper and broader knowledge of the inner workings of American intelligence across the board, a spectrum that might normally be the case. And in the process one hopes that they build up the collaborative and interagency information-sharing networks that I think we all would agree are very important in the post-9/11 world.

We were very thrilled to be able to recognize this effort led by our speaker this evening and to bring him into our distinguished group of award winners, much as we are pleased to welcome the leader of this innovation to speak with us this evening. But first, though, I'd like to turn the floor over to Mary Margaret Graham, who will introduce tonight's keynote speaker. Ms. Graham is a 2008-2009 Kennedy School Institute of Politics fellow, and most recently she was appointed as the first Deputy Director of National Intelligence for Collection in May, 2005. I just learned what "collection" means in this context and she will probably share that with you.

In that role, Ms. Graham worked on behalf of the Director of National Intelligence to conceptualize and manage oversight of intelligence collection programs across the whole of the Intelligence Community. Before that she has held many, many posts. She's served as Associate Deputy Director for Operations for Counterintelligence at the Central Intelligence Agency and in some 29 years with the CIA has had numerous field and headquarters assignments. She's also earned many prestigious medals for her service and I'm informed in just this year alone she was awarded the National Intelligence Distinguished Service Medal, the Distinguished Career Intelligence Medal, and the Secretary of Defense Medal for Meritorious Service.

So I can think of nobody better than Ms. Graham to introduce our keynote speaker this evening.

(Applause.)

MRS. MARY MARGARET GRAHAM (Fellow, Institute of Politics): Thank you, Tony. It is my pleasure indeed to introduce my former boss to you, the current Director of National Intelligence, Mike McConnell. I'd like to spend a couple of minutes and tell you a little bit about this son of South Carolina who is today both the President's chief intelligence adviser and the leader of the U.S. Intelligence Community – two jobs that keep him busy. He doesn't see much of his other half and I've been told reliably that she's complaining.

Admiral McConnell retired in 1996 as a vice admiral in the U.S. Navy after 29 years of service, 26 of those years as an intelligence officer. So he is a career intelligence professional, which is a rare breed sometimes in Washington. I first got to know Director McConnell when he was Director of NSA and I was booted out of the nest at CIA and sent to NSA to be the executive assistant for his deputy. And he was more welcoming of this operations officer than I had any right to expect. He was at NSA at a very interesting time because, of course, from 1992 to 1996 was a period when we were transitioning from what had been a bipolar world to the world we live in today – a multipolar world which, I think, we would all agree is replete with a multiplicity of dangerous challenges.

Before he was Director of NSA, he was the J-2. Now, in civilian speak that means he was the chairman of the Joint Chiefs and the secretary of defense's chief intelligence officer. And he did that during Desert Shield and Desert Storm. So he worked for General Powell, who was chairman, and for the current vice President, who was then secretary of defense. After he left government after those 29 years, he joined Booz Allen Hamilton and he was the senior vice President there quietly enjoying, I think, being in the corporate world when he got a phone call around Christmas of 2006. And I think it would be understating it to say that he had his arm twisted hard to consider the President's request to be second Director of National Intelligence.

And thankfully for those of us in this country and for those of us who worked with him every day, he did what he has always done. He said, yes. And he has been the Director of National Intelligence since he was sworn in on February 13th of 2007. I'd like to close with my memory of something he said to me early on when we were talking about collection and how intelligence collection in this world that we lived in had to be more dynamic than it currently was. He used a term that has stuck with me. He said, I need you to make sure that our intelligence collection capabilities can penetrate the seemingly impenetrable, and that really characterized for me

exactly the challenge that we faced. And that was to make these 16 – or try to make these 16 agencies work as one.

We are, I think he would tell you, still in the mode of intelligence reform in action. We've come a long ways thanks to his leadership in the last two years. We have a ways yet to go. But we couldn't have had a better second DNI than we've had in Mike McConnell.

So without further words from me, I give you Director McConnell.

(Applause.)

DIRECTOR MIKE McCONNELL: Thank you, Mary Margaret. Very, very kind words and I'm delighted to be back visiting here in Harvard and as you were introducing me, I was making up what I'm going to say.

Let me start by saying you reminded that I have a full day. When I first took the job and I was shocked at the hours and the requirements, I spoke in public maybe two weeks into it, maybe three weeks, and I remember the press article afterwards. I said something to the effect that I have a long day, I start at 4:00 in the morning and I generally try to get to sleep about 11:00 at night and I sort of described the day because it's an item of interest. And so the next day, the headlines said, New DNI Not James Bond. (Laughter.) Bad comb-over. Whines about his working hours. So I've learned to try to shape my remarks in a little different way to say it's a privilege to get up at 4:00 every morning – (laughter) – to serve the nation's interest.

One of the reasons I love to come to a new audience is I only have one story and those who've heard it before, they're wincing because they're going to hear it one more time. But when Mary Margaret mentioned the time when I served on the Joint Staff as the intel officer for General Powell, it was a fabulous experience. We went through a crisis period. We went through the collapse of the Soviet Union, so it was a fabulous experience.

Well, after that was over, I was privileged to be selected as a new Director of the National Security Agency and having a good, strong relationship with General Powell, I said what I really want to do is to have the general – everybody knew General Powell – to come to NSA to pep up the troops. And I called him and he said, Mike, you know how many requests I get a day? And I said, yes, sir, we're special, we've got this – he said, Mike, I've got a lot of special people. Just wait. So I kept – every time I would see him, I would ask him. I was looking for an angle, and finally I remembered he wore a uniform like this one right here, and if you'll notice these uniforms, they have lots of little buttons and – (inaudible) – I don't know where they keep the batteries, but they've got a lot of things up here.

Well, one of them is expert pistol and they have to qualify regularly. So I saw General Powell. General Powell, you haven't qualified and I have a pistol range out at NSA. (Laughter.) He said, okay, all right, you win. So I go down to get him. We're in this huge, black limousine going to NSA. The driver, Otis, is in the front. The general and I were in the back and we are going down the highway. General Powell is a person of action and speed. Otis, go faster. Sir, I can't go any faster. Otis, go faster. Sir, the last time you had me go faster, I got a ticket, I'm

losing my license. He says, I can't go any – he said, Otis, pull over. Otis pulled over. He said, Otis, get in the back. (Laughter.) So Otis and I are in the back; General Powell was up front, and we're driving.

We get to NSA and we were going a little bit over the speed limit and we go on to the post and the speed limit goes from 60 down to 25. We maybe reduced down to 55. Blue lights. Sergeant Smith comes out. You know, we got pulled over. The sergeant comes and looks at the car, says wait right here. He goes back. Now, I rolled down my window to see if I could hear what was happening. And the sergeant called in to the supervisor and he said, sir, I got a problem. He said, what's the problem? He said I've got a car that's doing 55 in a 25 zone. He said, you don't have a problem, give him a ticket. He said, no, you don't understand. He said, there's somebody really important in that car. He said, well, who can it possibly be? How can you be that important? He said, sir, I don't know who it is, but Gen. Colin Powell is his driver. (Laughter.) Wonderful experience.

What is intelligence? If I asked this audience, what is it? You probably would struggle a little bit. I saw a movie, I read a book, I know a little bit about it. But let me sort of break it down into parts for you and then I want to talk about the community and how it's vital that we have such a community and why it's such a challenge for the American people.

First of all, when you collect intelligence, there are esoteric parts of it that basically comes down to taking a photograph – take a photograph of military equipment or geography, or people, or something, but you capture something that you want to examine later on. People communicate and you can listen to that communication, intercept it, process it, know when it turned on, when it turned off, and you can get lots of information from it. Or you can recruit a spy. A spy is someone who will share information that's secret, that's privileged inside a government or an organization that will share it with you. Those are the basic building blocks of intelligence. There's other little esoteric pieces, as I mentioned.

So when you look at us as a nation, we have an organization that takes pictures from space, from airplanes. They use that to make maps. They use it to make foundation for the geographic tracking of the world. They look for weapons systems. They look for mobilization. They're always looking for information from the context of the photographs. We have an organization. It's called the NGA, the National Geospatial-Intelligence Agency. We have another one called the National Security Agency, the one I was privileged to lead. I will use an example that's historical: World War II.

In World War II, the great secret was that we were listening to and reading German high command communications from very early in the war. That was a strategic advantage that we enjoyed for the entire war. Now, think about that for a second. We are reading code to know what their orders are to the German field commanders. Often, we were reading it and understanding it before the German commanders could break it and decrypt it.

How do you now handle that information? Does the American public have a right to know? Now, think about the context. You're in global conflict, you're reading the communications of the enemy, and if it's compromised they'll change the rotors and their encryption system is gone.

And I've just introduced you now to the issue of sharing information and protection of sources and methods.

The primary responsibility that I have was that the new Director of National Intelligence is to cause these agencies – the three I've just mentioned – to share information across boundaries and at the same time protect sources and methods. If we have this very vital source of information that's allowing to either understand or intercept or have an appreciation for an issue that's vital to the country, do we want that to appear on the front page of the newspaper? So that's the dilemma we're always attempting to balance.

Now, let me give you a little more context. If you look at the history of intelligence, we're not very prepared for anything that's ever happened. It's because Americans don't like spies. Think about our Constitution, the framing of the Constitution, the framework of the time. It's expensive. If you think about spies in most of the 180 or so countries in the world, it's an internal police force used against its own people to keep someone in power. So when you think about it, it's not something that you want to embrace. So the history of the United States is we invent it when we need it and we built it up and then soon as the crisis is over, we take it down.

The first spymaster was George Washington. Invented his own encryption codes, ran his own agents. He was a spymaster, and a very good one. But as soon as it's over, you dismantle all that. Now, we went into World War II. We were not prepared and we had to build up two very significant capabilities. One is code-breaking; breaking the German Enigma code that I mentioned. Two brave Polish Army officers captured the machine, smuggled it to Sweden, smuggled it to Norway and smuggled it to U.K. and the U.K. was doing okay except they got more and more complex and they needed more brain power, more compute power. The United States of American invented computers in World War II to solve that problem and that early going is what we called the National Security Agency today.

The second thing is humans – humans that were willing to risk their lives to parachute behind the lines to run resistance movements to be able to resist what was going on. That's called HUMINT, human intelligence. So we did HUMINT and we did SIGINT, signals intelligence. So the shorthand in our worlds – SIGINT means you're listening to somebody talk, you're exploiting the fact that they're communicating, and HUMINT means you are among humans attempting to recruit a spy or run an operation in the resistance movement. That's what we did in World War II and we did it very effectively.

What did we decide to do as soon as World War II was over? Well, let's get rid of that stuff. Why would we need it for the future? Winston Churchill did us a favor. He kept coming up with clever terms: Cold War, Iron Curtain, bipolar world, threat of nuclear war. So we have a different paradigm. So the nation went through a debate in the late '40s and produced the National Security of Act 1947. In that act, for the first time the nation committed to an Intelligence Community. We created the CIA, the Central Intelligence Agency. They do HUMINT, human intelligence. And a DCI, the Director of Central Intelligence as the manager of the community.

Now, all the other resources were somewhere else and the DCI was managing as the Director of CIA, supposedly across the community, and that's how we're going to do intelligence for the nation for this thing called the Cold War. Well, what did we do in the Cold War? Mostly technology. We deemphasized HUMINT – hard to get agents to penetrate in a place like the Soviet Union. Denied territory. So what we did was invent new technology, technology that had never been thought of before. We captured high ground: space. We got up high and we looked down. Now, think about 13, 14 time zones of denied territory, can't get in, can't see, can't listen, no access. So we just went high and looked down. And so for the entire Cold War, the Russians could not think about, design, produce, test, or field a weapons systems that we didn't understand a great deal about. Usually all the countermeasures were built by the time they would field the equipment – incredible contribution.

We deemphasized HUMINT and we emphasized space and we also emphasized signals intelligence. That carried us through the Cold War. The Cold War ended and we all stood around and looked at each other and said, what do we do now? I won't try to make this too esoteric, but during that period, most communications were analog and at this end of the Soviet Union, the world became digital. The world became the Internet and the world became one global net. So you had a series of players that had been active for years and years having to go through a transformation – a new President, new priorities, what's the threat really, and so we debated.

And as usual, when 9/11 occurred, we were not prepared. We weren't ready because we had designed a system for a different purpose. Let me give you a couple of insights. The worry has always been if this global intrusive capability can listen to communications, how do we trust those guys? And our track record wasn't too good. If you look back over our history, the executive branch had used the community a number of times to conduct spying activities against Americans. It was wrong. The oversight wasn't sufficient and it was corrected in time. We actually had a period in our history where the chief justice of the Supreme Court back in the '50s had his telephoned tapped, as was one of the other justices, for what was supposed to be legitimate reasons, but it was not legitimate. That was discovered.

And I'll fast forward to a period of Watergate, when the community was used to do a lot of intrusive observation. Out of that came a bill called FISA, Foreign Intelligence Surveillance Act. Here was the dilemma. We need this large, robust, wonderful capability to protect us in the context of the Cold War, but we can't allow it to conduct any observation of U.S. citizens. And our wonderful democracy, we want it both ways. Don't let anybody bother us, make sure we're safe, but don't do anything to look at anything that might reflect my activity.

So the law in 1978 said okay to observe foreign, but if you observe anything in the United States, U.S. person for a foreign intelligence purpose, you must have a warrant. That was the law of the land, but it was an analog law. Where we found ourselves most recently is it's one global network. And so communications overseas by foreigners – terrorists plotting to attack the United States – those communications were passing through the United States. If you go back to the old analog law, it said if you take information from a wire, even though it's a glass pipe called fiber on a wire in the United States, you must have a warrant. So the dilemma for us was

we had a terrorist overseas plotting to attack us by speaking with a terrorist in another overseas location and the community was required to get a warrant.

The debate and the dilemma for us is how do you modernize that law for the modern age? And we debated. For two years we debated and we finally came to closure. The good news is when it was finally voted, two-thirds of the House and two-thirds of the Senate voted for it and here's what it says today: if it's a U.S. person anywhere in the globe, you must have a warrant. A judge must grant you to conduct surveillance and the purpose of the surveillance can only be for one thing, foreign intelligence. Now, why would you do surveillance of a U.S. person for foreign surveillance? What if it's a spy that's been recruited by a foreign agent and you need to know what they're giving away? You would then have a warrant for surveillance of that person for a foreign intelligence purpose.

The other part of the law is no warrant for a foreign target regardless of where or how you intercept it. And the third part of the law was in today's world it's digital, it's global – you can't do it without the help of the private sector and so the private sector was authorized to give us that help and provided a level of liability protection.

That's the kind of dilemma that we face in making sure we balance our responsibilities for conducting surveillance of foreign targets that might wish us harm and respecting the civil liberties and privacy of American citizens.

Now, I'm talking process. Most of you probably came to hear something about the substance of the current threats. The time limit is pretty tight on what I can say up front, so I'm going to leave a lot of that for your questions. But let me make reference to a public document that we just put out about two weeks ago. It's the trends document that we do every four years. We do it for the new President and it's published just before the inauguration.

What it says is that, on unclassified level, based on our research around the globe, here's our best guess for the next 20 years. And in that assessment which is unclassified, it's on the web at DNI.gov – you can go there and download it if you'd like to do so – it has some pretty alarming information in it. It says the threat of terrorism is going up. It says the residual terrorist threat will be around for a long, long time. The terrorist organizations are adaptive and resilient and determined. It says competition for energy. It says nation-states will probably have conflict over energy resources. It says water is going to go down in terms of availability. It says the price of food is going to go up 50 to 100 percent. Energy resources have become more scarce.

So as we face the future, adding weapons of mass destruction, to include biological, which is my personal greatest worry, we have a situation where we have a large community of professionals. Their responsibility is to track and understand those threats, to have inside understanding and prepare the Congress or the executive branch with sufficient information so they can understand, plan, and adjust the policy to confront those threats. That's what we do every day. That's why my day starts early. It is a privilege. It's quite a thrill for someone to be able to go in and sit down and speak with the President of the United States every day. We do it six days a week. The President-elect is doing it seven days a week. I don't know if there's a little competition there or not – (laughter) – but it's seven days a week. And the sessions last somewhere between

30 minutes to almost an hour. And the subjects are absolutely incredible. The speed with which these two particular gentlemen absorb information and move on is astounding. But we go through a great deal of substance on any topic you can imagine in the context of national security or potential threats to the United States.

So I'm delighted to be here and I look forward to your substantive questions. Thank you very, very much.

(Applause.)

MR. SAICH: So thank you very much for that very erudite exposition. Now, we come to the fun part of the evening. As you'll see, there are two microphones down here and there are two microphones up there. If people have a question they wished to ask, please come to the microphones and we will call on you in rotation to ask your question. There's very simple ground rules for this. You know who are guest speaker is, so we would first of all like to know who you are, so please identify yourself and where you're from.

Secondly, it's questions. It's not speeches, so please, one brief question per person, rather than speeches. And thirdly, as I always try to tell my children, a good question usually has a question mark at the end of it so that we simple folk know what you're actually asking us when it comes to this.

So please the floor is open. Don't be shy. I know it usually takes some time for people to warm up, so please come to the microphones we can make a start for this evening.

Yes, please, the gentleman here.

Q: Towards the end of your talk, you said that personally the threat of bioterrorism is your number one worry. But we're heard at the Kennedy School this morning some very doomsday scenarios of the chance being 50-50 of nuclear terrorism. So how do you assess the threat of nuclear terrorism in relation with bioterrorism?

DIRECTOR McCONNELL: It's captured better in the document that I made reference to that's available on the website. With weapons of mass destruction that could result in the death of many, many people – chemical, biological, nuclear – we assess biological as the more likely and it's better than an even chance in the next five years that an attack by one of those weapons systems will be conducted in some place on the globe – not necessarily in the United States, but somewhere.

The likelihood of nuclear, while we worry about it, and it's a major issue for us and we spend a lot of effort and time and resource in tracking it, is of lesser likelihood, but it's not eliminated. Now, the result, depending on once you get into the issue of what the weapons of choice might be, nuclear could certainly be devastating, but what we are beginning to understand is biological could have so much greater consequences. I'll just use an example: flu epidemic that the world had no immunity for in 1918. Fifty million people died. So you potentially can do that if it were weaponized and handled in the right way.

Nuclear, the more likely nuclear event would be radiological as opposed to a yield, but a yield is a possibility. Now, if Graham Allison is in the room, he has a different point of view and I would just refer you to his book because that book captures exactly what he thinks about the nuclear weapons – the threat.

Q: I'm curious what your view of the role of lawyers in the Intelligence Community is today and how it has changed?

DIRECTOR McCONNELL: Role of lawyers? Probably my closest colleague in the staff is my General Counsel. It's virtually impossible to do what we do without having a legal scholar and a lawyer involved in the process because it's a very delicate balancing act, as I mentioned. Something I mean to comment on I did not: it's my personal view that any large bureaucracy – any large bureaucracy – will redefine reality in its own self-interest. It has – however, it's established with role or mission or function or business or whatever, it will draw bounds and want to make itself survive.

Our track record on the Hill has not been stellar, so the oversight process to make sure that what we do because of what we do has to be intrusive, it has to be rigorous, it has to be engaged. And so once you start that debate, having a lawyer who understands exactly what the law says and how to make the argument in a legal context is essential. And so my general counsel is Ben Powell and he has been – I've probably spent more time with Ben than anyone else on the staff. So it's essential.

MR. SAICH: The gentleman up there?

Q: (Off mike.) I do research on the side about infrastructure attacks. What do you think the greatest threat to the United States in terms of cyber security and cyber threats?

DIRECTOR McCONNELL: Okay. Wonderful question. My view at the moment is the cyber threat is the soft underbelly of the United States. The reason for that is the United States depends on the cyber infrastructure more heavily than any other nation on Earth. Now, let me just give you a couple of examples. Financial infrastructure. Billions of dollars move around the globe, 24 hours a day. There isn't any gold in the bank to back up the transactions. There are no dollar bills. It's all an accounting entry. It's all based on confidence. So the vulnerability of an accounting system that's global, not adequately protected, is a tremendous vulnerability if someone's objective is to destroy data.

Now, I want to make a differentiation between: hacking, that's a nuisance; crime, it's a problem, but it's tolerable; exploitation, that's what foreign nations will do to steal information for competitive advantage; and data destruction. Data destruction is what al Qaeda would do given the capability. If they get into systems and destroy data in the financial system, how do you recover? Now, the financial community understands that, they've designed backups and so on. But broadly speaking across the nation, the things that are vulnerable are transportation, varying levels of commerce, electric power. All of those things are computer-controlled and it's built on a data infrastructure that runs essentially on the Internet. And you can sit and – half way around

the world and touch critical infrastructure in the United States, and so if someone understands how to get in and how to destroy data as opposed to just exploit data, it could be devastating to the United States.

MR. SAICH: The gentleman in blue.

Q: My question is about cooperation. It seems that in the past, before the attacks of 9/11, there were significant blocks to cooperation both between the Intelligence Community and law enforcement as well as with Intelligence Community of the United States and other countries. May I ask whether those obstacles still exist to that kind of cooperation because we've seen the results when there isn't any?

DIRECTOR McCONNELL: That quite frankly is the reason that my position was created. You recall my comments about a bureaucracy that will define reality in its school, competes with some other school, or you had a team as a Cub Scout or something, and culturally we want us to compete against them and there's always that tension between organizational groups. Legally, and I commented on it earlier, we defined our community as foreign intelligence and internal domestic and we separated it in the law. Foreign intelligence was handled one way. Title III handled internal. So we designed our own system to make the terrorists at 9/11 successful. If you're tracking someone who's a terrorist coming to the United States, once they're in, they're off limits to my community. Before 9/11, you had to violate the law for the law enforcement community to react.

So, one, you had bureaucratic resistance; two, we had a structure that put barriers between us. Since that time, the law's been changed, my position has been created and my mission is to make sure it's integrated. I would say it's a work in progress. One of the things that I focus on – and I've had this discussion in the White House at a policy level with the President – probably the most important contribution of the DNI, the DNI's office, is causing policies to be established and enforced that require information sharing, sharing of information across barriers.

Now, we've designed an infrastructure. We have an adjudication system. We know how to do this, but let me turn my hat around. Remember protection of sources and methods. If the equivalent of breaking German code is what we're exploiting today, what we did in World War II, how do I force people to share that information when it's so vital, if it's going to leak or be published or be compromised in some way? So we've addressed it. We've made tremendous progress. We're not finished with that yet. So I would give us a B, maybe even a B plus, but we'd still have a lot of hard work to do to cause the community to share across boundaries. And I meant to say this earlier and I thank you for your question.

There are six departments now. A department is headed by a cabinet officer. There are six departments and 16 agencies interspersed in those departments. So although I have cabinet rank, I'm not a cabinet officer. I have cabinet rank. I show up to the Department of Defense and say, let me tell you how you're going to promote people inside the Department of Defense so I can enforce information sharing. If you start that argument at the lawyer level, on the question I just had, you won't get very far. We had to start with the President and work down. This is heavy lifting.

So the President allowed us to redo our executive order which runs the community. It's called Executive Order 12333. If you're interested in the community, what it is and what authority, and so on, it's on the web. You can look it up. His direction to the cabinet officials allowed us to get there and it was a major move. What we're doing now is putting the implementation plans in place. That's why I say it's a work in progress. So it's much improved.

And I would one other feature. The primary mission of the FBI today is different from what it was before 9/11. The primary mission of the FBI is to prevent terrorism, prevent terrorist acts. The British made a decision years ago to have an intelligence domestic organization, or domestic intelligence organization – no arrest powers. We had the debate and made a different decision. We chose to give intelligence functions to people with arrest powers.

So it's a work in progress to bring an organization that's been around for 100 years into the Intelligence Community to behave as an intelligence officer, which is very different from behaving as a law enforcement officer.

MR. SAICH: The gentleman there in the back.

Q: One of the more prominent arguments after 9/11 in terms of assessment of what went wrong was the point made by many, I think – an overreliance on signals intelligence to the detriment of human intelligence. And I know that a lot of efforts have been made since then in the United States, but how do you see that balance now and where do you see it going? What kind of capabilities does the community need to improve on?

DIRECTOR McCONNELL: The reason I framed historical context in World War II, it was very strong in human intelligence and strong in signals intelligence, and it changed for the Cold War where we emphasized signals intelligence, as you mentioned. Because of that, we were mal-deployed for human intelligence. Recognized – the decisions were made, both policy and resource – change it. And so the upward vector has been very, very steep. Today we are significantly – significantly – more capable than we were at the 9/11 timeframe in terms of professionals, the training, training of an entire community. Many of the military services got out of human intelligence altogether. Now they're back in, in a very robust way. So training has increased, the pace has increased, and the capability has significantly enhanced.

MR. SAICH: There's a gentleman there in a T-shirt.

Q: Hi. Thanks for coming. Some commentators have said that the attacks in Mumbai mark a new episode and new tactics in the struggle against global terrorism. What's your view?

DIRECTOR McCONNELL: Well, I just remind that the attacks in India over the past few years have been stark. Last year 1,300 people died – 1,300 internal in India. This same group that we believe is responsible for Mumbai had a similar attack in 2006 on a train that killed a similar number of people, around 200. And if you go back to 2001, there was an attack on the parliament.

This is a burden for the democracies of the world – for us to cope with. Because a democratic systems that promote free speech and free movement and open discussion are incredibly vulnerable to someone who is willing to die in the context of being a suicide bomber or suicide attacker. So, I don't see it so much as new, but a continuation. If you examine the groups that we think are responsible, the philosophical underpinning are very similar to what al Qaeda currently puts about as their view of how the world should be. It's a continuation. If you go back to the trends document that I mentioned earlier, even if we are successful in tamping it down, organizationally and structurally, there is going to be some residual, so we are going to have to deal with this for a long, long time. So the balancing act for those of us in my business – how were we effective in penetrating and stopping something before it happens and still respect all the civil liberties and privacy issues that people are going to be very, very sensitive to? That's a challenge for us today.

MR. SAICH: Right here.

Q: My question was going to be moving on from the discussion on EO 12333. Would the ODNI benefit from more legislative authority in governing the 16 distinct intelligence agencies, and more so, like, would it benefit to make the ODNI a Cabinet-level department rather than an office of intelligence?

DIRECTOR McCONNELL: A fabulous question, and we've been wrestling with it since 1947. The question is do you want a Department of Intelligence? Now, if you're looking for a job on the Hill, Senator Bond would love to have you as a staffer because that's the question he asks me every time I see him. Here's the problem. We're conducting intelligence operations in the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Department of Homeland Security, the FBI. It goes on and on.

Now, if you're going to be a professional – I'll just take my example as Navy – I can't be relevant to Navy, I can't have credibility with the Navy unless I am of the Navy, so I go to sea with them, I understand the environment, I understand sound and water and submarine posture and so now I become a professional in the context of HUMINT and SIGINT and imagery and that sort of thing, but I'm relevant to the Navy.

So if I create a Department of Intelligence, how am I relevant to the Marine Corps or the Navy or the Coast Guard? So that's the dilemma. So we debated it and debated it and the decision so far is we're going to have intelligence units serve customers across the government. There are 16 sets of customers. And what we've decided is we're going to ask some official and give him a little power, budget, access to the President, IT, and policy, and say, make it work.

Now, are we making it work? I'll go back to the question have we solved all the information sharing issues? No, we haven't solved them but we're making progress. That's the decision the nation's made.

If I were to redesign it, I may have a little different structure, but the worry on the part of the agencies is we don't want that DNI guy to be operational. We don't want him to tell a law enforcement officer to go down to this city and knock on that door or to tell CIA case officers to

go to this city and try to recruit that guy. That's what they're paranoid against. As long as I control the budget and say, well, we want to recruit people, we want good work, and so on, that's okay. So the nation is not ready to go down the path yet of the way you framed your question.

Q: I'm an independent consultant for the Intelligence Community. In particular, I have a question about alignment, adaptability and agility, the three A's within the 2015 vision. Agility is almost an oxymoron or it's contrary to bureaucracy and large institutions, especially when you start to get into 16 different agencies and six departments. So the question I have is, how do you envision agility for the IC, and how do you actually – it's a tough question and I want to have a question mark at the end. I do. But I think it's a complicated one.

When you have that many players, if you compare that to a football team, you have an agile player, you know that he's quick and strong and fast. When you get into 16 different handoffs of people coming together and there's a fusion of a product or what have you, it's a completely different beast. And so I guess the question I have is, what is your vision? In 2015, you talk about agility, but what really does it mean? And are you there today and what really has to happen, because I see joint duty certainly helping. I see an intelligence university certainly helping, but at the end of the day, intelligence is really there to support decision-making, creating decision advantage, and really helping the operator.

DIRECTOR McCONNELL: Thank you for the question. Any spot on the globe, any crisis, we generally are delivering detailed and insightful information to a set of policy-makers as it happens with a full story at 6:00 – (inaudible). So when you live in the community, there's a level of agility that we've achieved. And as large as we are, as well resourced as we are, particularly when you understand – and I'll use Iraq as an example. When the surge occurred and we were able to not only have force, but we could have capability to persistently observe and to persistently listen and to turn those decision cycles in seconds instead of minutes or hours, it changed everything. So we achieved the agility for that focus. So that success was part of why we captured in 2015.

You have to be agile in today's world. I'll give you an example. To move \$100 million from Tokyo to New York takes about a second. Now, that transaction would be, hello, New York. This is Tokyo. I have a transaction. Hello, Tokyo, this is New York. I'm ready to receive. What is your transaction? I have \$100 million. I'm ready to receive \$100 million. Thank you, I got it. You're reconciled. Done. We've agreed. And now, you have electronic proof that that transaction took place. Both ends are satisfied. That took a second. Well, in our world today, if we don't think in those terms, we are not relevant. So that's why we say agility. That's why we strive for agility.

Now, there's another subtle part of agility here. We don't transition from one era to the next era very gracefully. We weren't ready for World War II that's why I teed it up that way. We did magic in the Cold War – magic. It was phenomenal what we did in the Cold War, but when it ended we didn't know what to do and we just sort of did what we did before. And so the idea is we have to always be on the cutting edge of the technology or the problem so that we're willing to adjust to it.

Now, we have a situation today where information is generated. We have a decision wherever it needs to be made – Defense, State, CIA, White House. It's decided and executed, and oftentimes that's a 30-minute cycle. So we are much more agile than people probably appreciate. We're global, but the idea is always be willing to task yourself to be more agile because you always have to be relevant to the current decision and today's decisions move at the speed of light.

Q: My question is about the definition of the U.S. interests in the past compared to what is likely to be in the future. And the reason I ask this is many of us in the world fear you actually. Reasons like the invasion of Panama to support the corporate interest like of United Fruit, regime change and putting despotic regimes in the Middle East, Africa, possible support to the assassination of people like Patrice Lumumba, who was the hope of Africa. As we got into the 21st century, where we have more common shared interest and common shared global challenges, where concerns like human rights, et cetera, probably bring us together, should we have less reason to fear you?

DIRECTOR McCONNELL: Yes. (Laughter.) If you look at the policy of the current administration or the policy of the incoming administration, it's based on freedom, democratic principles, respect for human rights – many of the things that you made reference to, some are illusions or real, some may have been real for a different time or a different purpose. I didn't catch everything that you made mention of. But the interest of the United States today is democracy, respect for human rights, and the right for everyone to be able to exist in the world in a situation where they're protected to pursue interests of their values and their family. That's why I say yes to your question.

Q: I've been taught that the function of intelligence is to provide decision-making advantage to policy-makers, yet history teaches that sometimes policy-makers don't have an appreciation for what intelligence – what the proper role of intelligence is. And sometimes the efficiency of an intelligence director is a function of his personality or his relationship with the President. What advice would you give for an incoming Director of National Intelligence to make sure that the Intelligence Community functions properly or effectively?

DIRECTOR McCONNELL: Well, first, I would offer advice to the policy-makers before someone who would replace me, and I would make some of the points that you just made. What I would argue for is this is a vital service. It has to be large, well funded, robust, apolitical, and responsive to policy needs, and I would provide lots of examples where that made a difference.

Now, having had the privilege as probably no other American, I guess, to sit across the table from the two candidates and talk about some really very difficult, hard problems, their perspective was remarkable when they really started to think about the complexity and the challenge and how would you work your way through this problem. And so both of the candidates at that time as we do this – we've done this many times with the incumbent President, all of a sudden had an entirely different understanding and appreciation.

So, one, I would argue professional community is going to service that policy-maker, but I also would say operational decision-maker and tactical decision-maker because this goes all the way

down – we often are supporting from the national level decisions that are made on the battlefield. We do that every day. So it's part of the job of the professional to make sure those who you are serving understand what it is and how they can be served. And it is a function of personality and relationship, more relationship than personality.

So I would make that argument to the incoming administration – already have. Whoever takes my place, if they are from the Intelligence Community, as a professional they already know what I just said. If they're not, I would make my best argument to make them understand the nuances of that. This is a come early, stay late, every day, seven days a week, never stop profession. That's what we do. If there's a crisis in the world that's brewing or a problem or an issue that's going to explode or a terrorist attack or whatever it is, that's our problem. We have to know about it, understand it, frame it, collect information and deliver it in a way that it can be a decision advantage for the policy-maker. So part of my charge is how do I cause the person I'm serving to understand that.

Now, I grew up in a service – the maritime service, Navy. I had an advantage. My advantage was I went to sea with my customer, so I had him captured. I could talk to him anytime, 24 hours a day, and we had a very uncooperative target that happened to speak Russian. It also wanted to be stealthy and secret and unseen. So my job meant I had to work it every day and figure out a way to make myself relevant to that customer. And quite frankly, it's not hard because they have significant challenges and they always want good information. And if you deliver good information, you're relevant, particularly if your information is better or more precise, more timely, or delivered in a way that is more useful to that decision-maker than the rest of the system.

Q: I just have a question that sort of picks up on your point about the way that bureaucracies often cultivate and us-versus-them mindset. Do you have any thoughts about the ways that that sort of healthy norms for how that trend, if it is unhealthy, can become better, whether in an academic setting like this one or within an agency?

DIRECTOR McCONNELL: I think it's a very unhealthy situation left unchecked. And my view is the framers of our Constitution whether they knew it wittingly or unwittingly, they captured magic. It's called checks and balances. Everything is accountable to something. We have a marvelous thing in this country called an election, so if the people are not satisfied with the current trend, we start over. My community has an accountability to a set of overseers in the executive branch, but I have to march to the tune of the Congress. They call, I have to go up there. And many times, it's not a pleasant exchange. Many times I'm listening more than I'm talking. And I'm being challenged in a way that is sometimes challenging for me to sit there and listen to, but it's making absolutely certain that what we're doing as an organization is serving the nation's interest consistent with law, consistent with our values, and so on.

So my view is any organization must have oversight – intrusive oversight in some way that there's accountability. In business, that's a profit margin with the board of directors and an audit in accounting system. Anytime it fails anywhere along the line, you get trouble. And I give you the financial crisis today. Our process of review and validation, when someone who couldn't afford a home could get a loan with no down payment for a home they can't afford to pay

interest only, to expect they're going to make money when they sell the house because the price has gone up, that's lunacy. So our system broke down. So my view is large bureaucracy, this is good. I'm redefining it to my advantage. So checks, balances, oversight is the only way that we'll check a bureaucracy, any bureaucracy: business, government, maybe even yours.

MR. SAICH: Time is marching on, so two last – last two questions.

Q: I just had a quick question. You mentioned the private sector briefly before. I just wanted to know what kind of oversight there is over the work you guys do with the private sector and do you think it's adequate.

DIRECTOR McCONNELL: There is intrusive oversight over everything I do. My money is appropriated by multiple committees for which I march and answer and provide information, and I have two authorizing committees. So if I sneeze and they don't like it, they could come have me explain why did I sneeze. So if I'm doing commercial or I'm doing a new law or I'm engaging in a foreign country, it's all subject to oversight – intrusive oversight. My approach to that is come on in. Let me show you. We have the law. We have a set of values. We have a set of regulations. Look at what we do. Examine it. If we're not consistent with something that you think we shouldn't be, then let's talk about it. And cause the law to be written in a way that we have bounds and there's an expectation of how we behave. And the amazing thing is that's how we behave. If that's what the law says and that's what the policy-makers ask us to do, that's what we're going to do as a professional organization. The U.S. military is the same way and I'm arguing that this community should be the same way: consistent with the laws and values of the nation.

MR. SAICH: I'm sorry. The time – (inaudible, off mike) – questions.

Q: In almost every good spy movie, they have a line somewhere where someone says that the public only knows when the Intelligence Community messes up, but 99 –

DIRECTOR McCONNELL: It's very true – very true. (Laughter.)

Q: But the vast majority of the time where they're succeeding in protecting the country, nobody ever knows about it. And so my question to you is, what should an engaged public be looking at to evaluate and oversee their Intelligence Community? How can we know whether the Intelligence Community is making progress in sharing information, is striking the right balance between protection and civil liberties? And on the counter side, how do we know when policy changes need to be made in order to allow you guys to do your job better?

DIRECTOR McCONNELL: Okay. The –

MR. SAICH: (Off mike) – if you want to roll in any concluding thoughts you may have.

DIRECTOR McCONNELL: Okay, thank you for your question. And there is the dilemma for operating a secret organization in secrecy for which the results are not shared. That's the dilemma. Before the issues of the '70s, Watergate and so on, there was limited oversight to this

community. Subsequent to that, at hearings, Church and Pike – Church-Pike hearings – wonderful reading if you want to go back and take a look at it – said we have to have intrusive oversight; established two committees: one is in the House and one is in the Senate. Now, those members are cleared. They can look at anything. They can challenge anything. Those members are your representatives. I have to do my work in secret.

And I want to go back to my example of breaking German code. If we're in a global conflict and we've figured out how to read their communications, and if they are made aware they can take that away from us, does the American public have a right to know, because my oversight committee knows and I'm doing this in the interest of the nation, and I don't want to compromise that source. That's the dilemma for my community.

So when I sit down and we have an oversight with my oversight committee, one of the things that I say in my warm-up remarks is you have a responsibility not only to oversee us, to protect us in a way that you explain to the American people: I am cleared. I have examined all this information and I can tell you that it's consistent with law, value, whatever. So the only way we've been able to come up with a system for a secret community operating in secret is oversight on the Hill.

MR. SAICH: (Off mike.)

DIRECTOR McCONNELL: Well, I'd just say thank you, again. They were wonderful questions. You are a kind audience. I anticipated maybe some going down a different track or two, but I did enjoy it. I hope it was useful to you. I found myself balancing between basic fundamentals of what is this thing called intel and some very sophisticated questions about nuances of our business. It is large. We are 100,000 people. We are global. We spend in the neighborhood of \$47 billion a year. We have a capability and a reach that satisfies the information needs of the President, the secretary of state, the secretary of defense, down to a soldier on the battlefield, and that's a very complex enterprise to operate. My role is to make sure it's integrated. We cross-train. People here are professional, and I get to be the briefer for the President each morning and that's the source of influence on all those other players.

So it's a privilege to do what I do. My time is going to run out pretty soon. I was asked to come back [in 2006]. I thought about it. Do I really want to do this? I wasn't convinced at the time that this was the right model. Now, we can make a decision to create a Department of Intelligence, and that's a different model, but where we are now is the things that we've been able to do are pretty astounding and the reason is I've got a relatively small staff. I wake up every morning thinking community, so we've got new laws, we've got new executive order, we've got new policies, we've managed the budget, and we're causing the community to be integrated like it's never been integrated before.

And the reason for that is I don't worry about running the CIA or the National Security Agency or NGA. My responsibility is the community and that's what I think about and that's what I spend my time on. So I spend 50 percent of my time becoming substantively smart so I can talk to the President, I spend 50 percent of my time managing the community, and I spend 50 percent of my time dealing with the Congress. (Laughter.)

So thank you all very, very much. (Applause.)

MR. SAICH: Let me just thank the Director on behalf of everybody. He ranged across a whole lot of issues, and I thought it was fascinating – the question, the balance between information, information flows, access, and the question of national interest, questions of lawyers, whether in fact we should be fearing the U.S., and also other issues related to this question of not only the integration within the agencies themselves, but also the relationship to outside contractors.

So please, let's thank again the Director for spending time with us this evening.

(Applause.)

(END)



Director of National Intelligence, Mike McConnell, addresses the John F. Kennedy Jr. Forum at Harvard's Kennedy School of Government in Cambridge, Massachusetts. (December 2, 2008)