Remarks and Q&A by the Director of National Intelligence
Mr. Dennis C. Blair

U.S. Chamber of Commerce
National Security Task Force Meeting

Washington, DC

July 22, 2009

MS. ANN BEAUCHESNE (U.S. Chamber of Commerce): Well, good morning, folks. We're going to get started. I'm Ann Beauchesne. I'm Vice President of National Security and Emergency Preparedness here at the U.S. Chamber of Commerce. Welcome. The chamber is incredibly pleased to have Director Blair join us this morning to discuss the direction he will be taking American intelligence.

Before I introduce the director, let me just say a special thanks first to our sponsor this morning, Tom Donohue, Jr., of Adelphi for generously supporting this morning's meeting. Without support from our members, we can't do briefings like this so we really appreciate it. I'd also like to especially acknowledge the partnership, collaboration and friendship that Linda Millis and Lori Feliciano of the ODNI's private sector office have shown me personally, as well as all our members. We really appreciate the support they've given the chamber.

I'm not going to read the director's bio. You have that at your desk. Let me just say that in passing the Intelligence Reform and Terrorism Prevention Act of 2004, Congress approved the most comprehensive reform of the U.S. Intelligence Community since its establishment over 50 years ago. Principal among the enacted changes was the establishment of the Director of National Intelligence – the DNI – to manage the Intelligence Community. And I think Director Blair would agree that the DNI position is not only one of the most important positions in town; it's also one of the most challenging positions in town.

As you all know, Admiral Blair became the nation's third Director of National Intelligence this past January. This morning, he is going to highlight some of the specific intelligence issues he's been focusing on, such as violent extremism, WMD proliferation, threat warnings, cyber-security and counterintelligence, information sharing and the importance of the public-private partnership. Director Blair's going to speak for a few minutes and then he'll take your questions. And we'll go to the Chamber members first and the press following that.

And I just want to say that we had the opportunity to visit with the Director last week and got to tour the National Counterterrorism Center out in McLean, and he said that they're in the business

of stealing secrets. And we know he does much more than that. So please give a warm welcome to Director Blair.

(Applause.)

DIRECTOR BLAIR: Oh, thanks very much. And it's a pleasure and an honor to be here and to have a chance to speak with this impressive group of business professionals. Now, I spent a little time – if you read my biography – in the United Kingdom for a post-graduate degree. And while the United States does have the best Intelligence Community in the world, the Brits have an excellent one, too. They're a proud nation. And one influence not only on the police detectives of the United Kingdom and many other countries but also on their intelligence officers was Sir Arthur Conan Doyle, the author of the famous Sherlock Holmes stories.

As we look at this intersection between business and intelligence, it's worth telling a little story on Arthur Conan Doyle. Supposedly, he was coming into Paris. He hailed a cab, threw his bag inside the bag, climbed in and before he could say a word, the driver said to him, "Where to, Monsieur Conan Doyle?" "You recognize me?" he said in surprise. "Non, never seen a picture of you." "Then how do you know I'm Conan Doyle?"

The driver replied, "I read it in the newspapers that you're on vacation in the south of France. I noticed your train came from Marseilles. You had the tan of a week on the Riviera. From the ink spot on your right middle finger, I deduced you were a writer. You have the keen look of a medical man and the wardrobe of an Englishman. Putting it all together, I felt you must surely be Conan Doyle, the creator of the famous Sherlock Holmes mysteries."

Conan Doyle was amazed. "Extraordinary, my good man! You are yourself the equivalent, the equal of Sherlock Holmes in your powers of deduction." The driver said, "There is one more additional fact, monsieur. Your name was on your valise." (Laughter.)

So I guess in every business, in every time, every country, people have something valuable to contribute to what we call intelligence. And quite often, many of the important things are not so secret that they aren't even hidden.

Now, one question you might be asking yourself even despite reading my impressive biography is how I got this job. (Laughter.)

And I must tell you it wasn't a typical story. Before the election of last November, I had a grand total of one conversation with then-Senator Obama. Now, I was very impressed by him in that conversation back in 2006, and apparently, he remembered me. But I was, at any rate, quite surprised to receive a phone call the day of the election asking me to join him team. I had to have a serious conversation at home before I accepted, but Diane says that she thought it was extremely important to continue to try to serve the country. I was very impressed with the President-Elect's vision for the country, so I was happy to take on the job.

Except for some time at the very beginning of my career as a collateral duty intelligence officer on the USS *Barney*, my first guided-missile destroyer, then a tour as the first Associate Director

of Central Intelligence for Military Support back in the mid-'90s, I was primarily a demanding and somewhat dissatisfied consumer of intelligence.

But I've always had great admiration for those who collect intelligence, those who analyze it and those who try to help decision-makers and other officials do their job by telling them what might be going on, on the other side. Any military commander can tell you that intelligence is extremely important to doing a good job. And so, do, to ambassadors and policymakers, development workers, trade negotiators – all those who are representing this country and its interests.

I did suspect before I took the job that the Intelligence Community could use some more work to become even greater than the sum of its parts. And I've become a truly firm believer in that aspiration. I've seen firsthand that the integration of the various effective parts of the Intelligence Community produces amazing results that none of them can achieve alone. And really the essence of my job as a Director of National Intelligence is to weld those pieces together, so we can have more of this integrated action as we carry out the nation's business.

In addition to my office, there are 16 organizations that comprise what we call the Intelligence Community. They range from separate agencies to bureaus that are inside of other departments. And altogether about 100,000 people – military and federal civilians – get up in the morning and go to work in this Intelligence Community. The larger organizations are fairly well-known – the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, the Federal Bureau of Investigation. These last five come under the – in addition to reporting to me – come under the Department of Defense and the Justice Department.

And there are 10 other organizations with substantial intelligence arms that are also part of this team. The DEA falls under Justice also. The Army, Navy, Air Force, Marine Corps all have large military intelligence components who come to my executive committee meetings every couple of weeks. The Coast Guard comes under the Department of Homeland Security, and the Department of Homeland Security has its own intelligence section as well. The Departments of State, Treasury and Energy each have also important intelligence offices.

So as you can imagine, this diversity makes for a very complicated organization chart, and puts a premium on working together. But there's a tremendous range of skills and expertise that we can draw on in order to try to support policymakers, and support action in the field.

It was exactly five years ago, July 22, 2004, that the 9/11 Commission issued its report. And one of its recommendations was that all of our intelligence elements needed to be better integrated. And that was really the genesis of the action that five months later resulted in Congress passing the Intelligence Reform and Terrorist Prevention Act – that act that created the job that I now hold, Director of National Intelligence, once the President signed it into law.

Now, that job essentially gives me three roles. The first one is as head of the Intelligence Community. It's comprised of those 16 agencies, 16 components that I mentioned. And leading that community entails setting priorities and providing leadership on the cross-cutting issues that

affect more than one of those departments. I try to align the incentives, I enforce compliance, and that's done to coordinate how our community will address issues that cross the boundaries that none of them can do alone, that they all must work together in order to accomplish.

I can and do issue policy directives that are binding across the Intelligence Community. I clarify roles and responsibilities, and that's especially important for any policy that involves collaboration. And the really important ones all do.

Another important part of leading the Intelligence Community is supporting the field operations. Right now we have diplomats, military units, reconstruction teams working in Iraq, Afghanistan, Pakistan and elsewhere around the world. We have CIA teams, military units that are combating violent extremism. And providing support for all these units in the field is a key job of the Intelligence Community; and we do it very, very well. The sort of precise, tactical-level intelligence to those in the field is eye-watering now, and it's much greater from the days that I can remember being a junior officer, a mid-grade officer in the field. We really give our units an unfair advantage, which is what they ought to have.

My second role in this job as DNI is as the principal advisor to the President on intelligence matters. Yes, I'm responsible for his daily morning intelligence brief. I serve as the top intelligence advisor on the National Security Council, but it's really much wider than that. I'm responsible for the intelligence that informs the entire national security policymaking process that begins with interagency groups, and proceeds up in a hierarchical set of meetings to the National Security Council deliberations themselves.

And I meet regularly with the Congress, providing them with intelligence knowledge of what's going on in the world. They, of course, provide the budget and the oversight for our community, and I can't emphasize how seriously I take that relationship as well. In fact, this afternoon, I'm having a long meeting with the House Permanent Select Committee on Intelligence. I've been on the phone with Congressmen over the last couple days. This is an extremely important partnership that we're working very hard on.

My third role as DNI is to manage the National Intelligence Program, with its budget that's in the tens of billions of dollars. We publish it retrospectively at the end of each year, and it's a lot of money. And it's an important job to make sure that these resources are apportioned correctly across the Intelligence Community, so that they give us a balanced program, so that all 16 of those agencies can play the proper roles in achieving the national intelligence priorities that cut across all of the individual organizations. And that putting together that budget, both within the executive branch for the President's approval, and then justifying it to the Congress who authorizes and appropriates it, is an extremely important part of this job.

Now, underlining all of these three separate roles is really the responsibility to make sure that the Intelligence Community is coordinated and integrated, that we really do connect the dots. And as I've said, it's clear to me that in doing that process, the Intelligence Community can and should be greater than the sum of its parts. That's clear to me, but I want to make it clear to you who have some knowledge of the Intelligence Community. And I certainly want to make it clear to the American people who we serve, and who support us.

Now, some of this alignment, some of this connecting the dots does occur naturally. We've got smart people, been in the business a while – they can reach out to make things happen. But it does require effort from the top, the kind of alignment that I talked about, in order to increase our shared effectiveness, to reduce overlap, and to use our precious resources on the most important jobs in the most effective way.

A whole separate aspect of becoming effective as an Intelligence Community is to make more use of the talents and expertise available in the private sector. In fact, of course, working with the private sector is as old as the Intelligence Community itself.

We've always depended on private expertise, resources and know-how. Corporations, academics, nongovernmental organizations have built many of the tools that we have needed and used, and they've taught us ways of looking at issues which are important to understanding.

It's the private sector that provides the critical infrastructure. And our country literally depends on you and the companies that you represent for the Intelligence Community to reach its full potential.

So I'd like to acknowledge the Chamber's previous support in this area in reaching out to my predecessors. You in the Chamber, and this task force in particular, have been key supporters to our early efforts in engaging the private sector. We've had workshops; we've had the DNI-CEO summits in which Cabinet-level officials have participate. Just last week I was privileged to host the Trade Association Partners meeting.

In particular, Ann Beauchesne, Matthew Eggers, Tom Donohue have all been instrumental throughout this organization in building some of these bridges; helping us identify the member companies, the key leaders within the business community, to participate in this on-going dialogue. So thank you, Ann, Matthew, Tom. And I think a round of applause is really in order for all of them. (Applause.)

We know it hasn't gone as fast as everyone would have liked; and I'd like to change that, to speed up the pace. In the phase that we really are now in this effort, we're trying to move beyond outreach – which is a critical first step – to really move to partnerships; partnerships that are defined by a shared sense of mission, shared responsibility. And this takes a while, but once we reach this step, I think things can really take off.

We've made tremendous progress sharing intelligence within the government. We've worked hard to improve transparency with our foreign partners. We've taken steps to be even more forthcoming with others. We've worked with our communications within our partners in the United States – homeland security officials, law enforcement officials – at the state, local and tribal levels.

In fact, we just held a big conference about that recently in my headquarters. And I was pleased that all the participants there – representatives of the associations of many of these law enforcement officials – feel that we're making good progress there. And we're having a better

understanding of the roles that we each have, getting good ideas together and making a better team.

In academia, we have partnerships where several universities are getting five-year grants, averaging over $250,000 a year, to develop courses and produce graduates that meet our hiring needs. Many of our academic partners have substantial minority/ethnic student populations. And that's by design that we are working closely with those institutions, because this world is changing. We need an intelligence workforce that reflects those changes, and that can help us with the many different challenges that we face in the intelligence world.

But it's really the business world, that you all represent, that may be the last frontier in many ways in building these partnerships – except for course, that about a quarter of our workforce is made up of contractors, so that has been a way of connecting in the past.

But while we have contracts and while we have contractors working with us, we really have to go beyond that, I think, to real partnerships where we really understand each other, ideas are coming up from both sides, there is a natural collaboration, and we're getting the job done for the country.

We sometimes describe our future Intelligence Community as an enterprise, and that's the vision that we can achieve when we're totally integrated, agile, and exemplifying this country's values.

So what would be different? I think one way of thinking about it is that today's Intelligence Community would be the nucleus of intelligence professionals. We are the ones who get to wear the spiffy badges every day; we work in the vaults where we can't take our cell phones; we have to endure polygraphs. And the community is defined in law; and that will continue to be the center of this enterprise.

But in the future, we have to include a larger membership. And think of it as an electron cloud surrounding that nucleus. Our close allied foreign intelligence partners are in the enterprise.

As I mentioned, academics, think tanks, often, outside experts can be brought in for specific projects and provide enormously valuable insights and additions. And then we can bring in commercial and private sector partners, also, to leverage our efforts.

We need to be able to partner with these groups in ways that complete our missions; that give us all the tools we need to do each of the jobs. And we can't do that alone. We not only can't afford it, but we can't get the people.

So in order to form these partnerships, we have to answer a basic question: What do you, our partners, want? What do you need to be able to work together with us in a way that is to both of our advantages?

We know you need access to information. Expertise – we need it coming in your direction. So it's really a case of finding out what the mutual requirements are, concentrate on the mutual mission, in order to be able to get the job done and to make this enterprise as great as it can be.

There will always be an element of secrecy in our profession, but I don't think there has to be so much an element of mystery as we currently have. Much of our job is straightforward: We try to steal the secrets that our enemies seek to keep from us. But secrets alone aren't enough to support policymakers and American officials and fighters on the field. A huge amount of the information that's both available and extremely important is in the open – Conan Doyle's name on his valise. The trick is to meld the two together in order to answer the mission requirements.

So we'll continue to be asking for the expertise of the private sector. We truly want to develop an appropriate and mutually beneficial relationship providing real opportunities for our partners. And I guarantee you, they will always do this in a way that pays close attention to protecting our privacy and the civil liberties of Americans when we take these steps.

One mega trend that we all deal with, that really brings these issues into relief, is the growth of information technology, and it's happening in the private sector, it's happening within government.

For our intelligence analysts, it raises real challenges as well as opportunity to sort through the huge terabytes of it – or even petabytes of it – I didn't even know such a word existed until a couple of months ago – but to sort through all of it to find out trends, to find out what's correct, to find the invaluable individual pieces of information within the mass of information that's out there.

The Internet is a source of information invaluable to all. The trick is to sort out what's true from what's false. And the trick is also to do it in a way, as I mentioned, that is consistent with American values, and protects the civil liberties and privacy of the citizens of this country.

Many of the tools of the IT revolution have helped us in that sorting process. And networks themselves are crucial to our operations in a way that I'm sure you all are familiar with in the businesses that you run.

And in addition to bringing tools, opportunities and information, they also bring vulnerabilities. The President has declared our cyber infrastructure – our communications and information technology backbone – as a strategic national asset. And protecting that asset is a national priority. The threat to that backbone, to that infrastructure, comes – yes – some from nation-states, but also from various non-nation-states, and even individuals who seek to harm it for various reasons.

Now, I don't believe the United States is at risk right now in the way that we have seen countries like Georgia and Estonia attacked recently. Our infrastructure is too big, it's too complex, we have practice dealing all the time with a serious number of attacks and other obstacles, so I don't think we're in that sort of vulnerability. But as you look out in the future, unless we continue to work hard on it, we could be very vulnerable. So we are taking this seriously within the Intelligence Community as one of our missions.

As you know, the public and private Internet networks are very intertwined. We use some of the same cables, same service providers, same switches; and we need to work hard to ensure that we're understanding and working together on what's going on in the Internet. We have to know how to protect our government and military networks from being penetrated. And at the same time, we need to share ideas so that American business can use them in their work in protecting private networks, and we can take advantage of their experience.

The Department of Homeland Security has the primary role in protecting American citizens from cyber events and protecting the critical infrastructure on which our country depends. And they have the appropriate statutory responsibilities, and we coordinate with them very, very closely.

And one of the most important government agencies in this respect, which works with the Department of Homeland Security, is the National Security Agency. My personal belief is that we need to use the NSA's technical capabilities to better protect American networks, both in the network and this critical infrastructure that we depend on in so many ways to lead the life that we lead – the electrical grid controls system, financial networks and many others.

But again, an important caveat is that we must do all of this while being consistent with the protections of privacy and civil liberties of our citizens. Americans must have confidence that the intelligence is being used only to save lives and protect our nation – which is, in fact, the case – that it's not being used to gather private information about Americans. We need to reconcile this use of expertise with some of the public perception.

So it's my responsibility to make the case to the American public that we can do our part in protecting the federal networks and protecting the civil liberties and privacy of Americans; to make the case that we'll cooperate with those who are protecting the private networks, that we'll do our jobs carefully, under supervision, entirely within the provisions of the law, and with proper oversight from both the legislative and the judicial branches.

One of the things that I've really been most impressed with in the six months I've been on the job is the teamwork that's developed between these different agencies that are in the Intelligence Community, and the teamwork with other agencies of government. The integration will be just phenomenal. Often, a team figures out how best to integrate all on its own – happens naturally – it's wonderful. And we just cheer for that. They have members who specialize in human intelligence, signals intelligence, geospatial intelligence, other areas. They come together, they know what their mission is, and they're able to produce incredible insights on it because of their individual expertise and the teamwork.

This is a microcosm of what can and what should happen for the Intelligence Community at large, and in fact, for this larger enterprise that I'm talking about that includes private sectors, whether they be business or academia or think tanks or NGOs. We need to be agile in order to form these relationships, to be able to understand a world that is increasingly fast-paced and complex. Our workforce has to be diverse, professional and mission-driven. We need to embrace innovation, to take appropriate risks, to encourage initiatives at all levels. And this enterprise that we build must exemplify American values.

You may have heard that the Partnership for Public Service recently selected the Intelligence Community as one of the best places to work in the federal government. And I think that's especially remarkable when you realize that half of our workforce has joined since 9/11. They are largely a group who's been inspired by the patriotism that flowed out of that event.

I don't think our community is quite as widely known in the country as it should be. There are three really highly respected professions in America who serve this country or their communities, and that go in harm's way to protect their fellow citizens: the armed forces – soldier-sailors, airmen, Marines, Coast Guardsmen; police officers – federal, county, state or local level; and first responders – firefighters and other first responders.

But I think we also have a fourth group who protect their fellow citizens and also put themselves into harm's way. Unfortunately, they often receive little praise. They're not generally considered in that group that I talked about, and they're sometimes even viewed with suspicion by their fellow Americans – and these are the members of the Intelligence Community.

Now, most of them are not case officers risking their lives recruiting foreign agents, just as most police officers are not on the SWAT team and most armed forces are not Navy SEALs. The vast majority go about their job doing things that are perhaps not as glamorous, but that are part of that integrated team that produces the results that I've talked about – the results that protect this country and the results that support the interests of the country. And I think that over time, we can make Americans just as proud of this Intelligence Community as we can of those other groups that I mentioned. And that certainly is my goal as a leader of the community.

I'd like to finish with some words from the American poet Emma Lazarus. Coincidentally, July 22nd, the day on which the 9/11 Report was produced, is also the anniversary of the birth of Emma Lazarus. It's her 160th birthday.

And she wrote a poem that is in a very important place. It's engraved on the Statue of Liberty in New York Harbor. And it reads, as those of you who have visited it or read about it know:

"Here at our sea-washed sunset gates shall stand
A mighty woman with a torch whose flame
Is the imprisoned lightning, and her name
Mother of Exiles. From her beacon-hand
Glows worldwide welcome; her mild eyes command
The air-bridged harbor that twin cities frame.

'Keep, ancient lands, your storied pomp!' cries she
With silent lips. 'Give me your tired, your poor,
Your huddled masses yearning to breathe free,
The wretched refuse of your teeming shore.
Send these, the homeless, tempest-tossed to me,
I lift my lamp beside the golden door!'"

We in the Intelligence Community feel we have real responsibilities for this country that Emma Lazarus wrote about, and the people who came to it. We gather the information to protect it. We hunt the successors to those who brought down the World Trade Center, which lies a short distance north of that Statue of Liberty.

We watch the world for threats and for opportunities, reading images from satellites that fly high over this Earth; talking to sources in dusty alleys in dangerous, distant lands. And beyond working on today's problems, we're thinking hard about the problems of the future and investing in the future.

We want tomorrow's intelligence professionals to be even more highly skilled than we are, to have tools that are better, to work as an even more tightly integrated team than the Intelligence Community of today. And we clearly want to have a better partnership with you in the private sector, who can help us in so many ways.

So let me turn this from a talk into a discussion, hear what your ideas are, and we can take a few questions, I think, Ann.

MS. BEAUCHESNE: Very good. Thank you, sir. We'll start with a few questions?

QUESTION: Director, thank you for your comments. One point I'd like to ask about in the partnership, I see sort of two areas: One is the critical infrastructure in our private sector networks which – I think it's absolutely essential that we work more closely with you in the Intelligence Community because as many people are trying to get into our networks as are trying to get into your networks.

But I'd like to ask a second question in terms of a partnership. And one of the things that many of us in this room love about the American business community is innovation and creativity and new ideas and new solutions. And the question I have to you is, while we look at our existing networks and the security of those networks and people that are trying to penetrate them, how does the business community, which lives and dies every day by innovation and new ideas and new products?

How do we become a better partner with you as you start looking at working through all of this data, looking at new ideas, looking at new ways to protect things and how does the business community bring the innovative ideas that we're developing in our core businesses to do a lot of other things and help you become better at your job? And what are the things the business community should be doing in terms of bringing you ideas, or getting questions and needs from your community, so that we can put minds and creativity and capital to those solutions, so you don't have to do it all yourself? So I guess that would be my question.

DIRECTOR BLAIR: I think there's not going to be one answer to that question, Tom. If we simply are relying on the old RFP process, we're going to miss most of what is going on. As I mentioned in my remarks, I think it has to be a much richer dialogue than that. And I think that we don't know the new answer to your question, so we have to try a bunch of stuff.

Some of the – one of the new things we're trying, as you know, is IARPA, the Intelligence Advanced Research Project Activity (sic). And one of the key focus areas for IARPA is exactly on information technology. And that is quite an open architecture approach to projects. I mean, Lisa [Porter, Director of IARPA] and her people will do everything from just talk to somebody and encourage based on a conversation to looking at papers, to a whole ways in between.

So that's I think one key thing in the really cutting-edge area. I think an important part of that also – especially in the IT area – is, is there a tolerance for experimentation and knowing that, you know, not everything is going to work 100 percent, but we need to try ideas and work them in? So IARPA is one thing I would point you towards.

Another area of outreach is in our science and technology directorates, where we are trying to have a series of forums with industry to be able to have that sort of frank discussion. We can get engineers talking to engineers, as well as, you know, written requirements and come up with the ideas there.

At the higher levels, our Enterprise Support Group, the ESG, which has the CEOs of IT companies meeting with me and other government officials, we have not had a meeting since this administration started, but I intend to kick that back in, so that we have contacts at the very highest levels and we can follow up ideas.

We have our Intelligence Science Board, which also has a number of representatives representing both academia and private IT companies that can do it. So I think that more is better in this case, and we just have to work all of the different angles we have.

I do know that on the, you know, strictly IT insurance or IT protection companies to government, there are well-established trade relationships to make sure that we're comparing notes – often through the CERT teams and so on, on particular techniques, particular viruses.

But I think you're talking a little bit wider than that, and I think we need to open that. So I haven't gotten a report from last week's conference, if any new ideas came along in that regard.

MS. BEAUCHESNE: No, we'll get back to you.

DIRECTOR BLAIR: But I think that we should look for them. But thank you.

MS. BEAUCHESNE: Other questions? There are microphones around the room. We'll go to the press after. Let me just get the audience first. Yes, if you could go to the microphone and identify yourself too. Sam, there is one right next to you.

QUESTION: It seems that the cyber discussion is focused on domestic issues: securing dot-gov, dot-mil, the defense industrial base. But it would also seem to some of us that there is a global interest, that the United States needs to play a global leadership role in terms of global cyber governance, that there are global supply chains, global critical infrastructures.

What might the government do better to begin to build an architecture of U.S. leadership in global cyber governance? And how can the private sector help?

DIRECTOR BLAIR: I think that's an accurate observation, Sam. I would tell you, frankly, that in recent years, I think we have felt a little bit of overconfidence in the American nature of the Internet, and that sort of thought that we will set the standards for it and not really focus on these global bodies, who in fact are setting up those protocols and many of the procedures which have an effect.

And I don't think we've been as strong with the teams that we've sent to those conferences with the positions we have going in. And, as you know, that's a State Department lead responsibility. We in the Intelligence Community provide some support, but I would think that that would be an important place for American computers, switch, cable, software manufacturers, to really focus on, to make sure that, as a country, we have our act together with the sort of standards, protocols and international agreements that are facing us. So I think that's one very important one to point to.

If you look at the story in China, for example, a huge number of computer users, a country that is, you know, if it could write its own ticket, it would write it all with Chinese leadership in designing the Internet across the board.

If you look at what has actually happened, though, China has to play in the international game and many of their preferred domestic solutions have not won out over international – sometimes American, sometimes other – positions. So I think that the IT world is open enough and developing enough that good ideas – and a lot of these are American and a lot of these are right for us – can be the ones that still set the pace globally.

I think we have natural allies in many countries that we have worked with traditionally, but they don't come without work on it. So I think you're pointing to a very important area. I think we need to not only work with the President's cyber coordinator in the White House, once he or she is named, but really get our act together on these international delegations that negotiate these things.

MS. BEAUCHESNE: Yes?

QUESTION: Admiral, thank you for coming to address us today. The National Counterintelligence Executive's office in their report to Congress identified some 108 different countries, friend and foe, that are actively and aggressively stealing technology from the United States. How do we work with the government to get an understanding in the Intelligence Community that the government can help us, can work with us and can counter some of these issues?

We see the DOJ has, since 1996, with the Economic Espionage Act, only done a couple of economic espionage cases because it doesn't meet their threshold. How about we get consistency across the country to protect the infrastructure so that the economic security of this

country becomes as critical of an issue with the Intelligence Community as the national security issues are? Thank you.

DIRECTOR BLAIR: And that comes right before world hunger and – (laughter). It's very important. I think we still have this tension between attribution and enforcement on the one hand, and warning and protection on the other hand, in the cyber area. And we haven't really quite figured out the right area.

You know, the law enforcement world operates on the premise that if you catch a few criminals, you generally deter the rest, and there's enough law and order that life can go on. When you apply that philosophy to – I'm not sure if you can apply that philosophy to cyberspace directly, where there seems to be an unlimited number of both nation-state actors and non-nation-state actors trying to steal secrets and cause havoc over the net. And I'm not sure if catching one or two will deter all of the rest.

So while we are catching those we can, by the very careful process of attribution of an attack, working through law enforcement agencies, we have to get this warning function out there that this is the vulnerability that was used in this particular attack; those of you who have a similar server or similar software or similar vulnerabilities need to work on them. And we need to be able to do both at the same time – to be able to prosecute and attribute at the same time we're fixing and patching.

And I think the evolving partnerships among the computer readiness teams – the CERT teams, the FBI team, the DHS team, the teams that we have on the intelligence side, the private center up at Carnegie-Mellon – I think those are getting better in that regard, but I still see instances in which vulnerabilities go on for a longer period of time than they should have, when we actually know something either on the intel side or on the law enforcement side that could have helped others patch the vulnerability quicker.

For instance, in some of the budgeting that's before the Congress right now, there's increased funding for connections among these centers, so that they can be better connected in real time as one of them works a problem to pass around the technical knowledge on what was the source of that attack, and so that they can publicize it in the various ways they have within the government and within the private sector, so that patches can be put in, other vulnerabilities can be addressed.

So I guess my answer to your question right now is better connection among the operation centers and the cyber-security centers, earlier decisions on sharing information while we're prosecuting and attributing attacks, and then a greater level of technical interchange among those areas. I think that's the way we have to approach it.

MS. BEAUCHESNE: Thank you. Other questions?

QUESTION: Thank you. An observation and then maybe a question. You've had critics, mostly from Capitol Hill, complaining about the size of your organization – ODNI itself. I'd like to hear, if you wouldn't mind sharing, what your plans are to get them – them, the Congress – to be actually on your side and helping you understand your value-add for the community.

Secondly, you mentioned that 25 percent, I believe, of the workforce that you oversee is contracted out. And there have been critics about that as well. Obviously, the private sector can provide you and does provide you with flexibility – been able to respond quicker bringing on contract employees – and faster, I hope – but is there a magic number that you're looking for or anybody's looking for as far as a mix between federal and outsourced resources? Thanks.

DIRECTOR BLAIR: You know, those are very good questions. On the size of the workforce in the Office of the Director of National Intelligence, I think it's important to understand that we really have two separate categories of workers. We have interagency centers, many of which existed before the creation of the DNI, who are doing real operational work.

The largest of these is the National Counterterrorism Center, whose predecessor, again, existed before the DNI, but was expanded in very important ways with a large influx of FBI officers, in addition to CIA officers, in addition to other officers in the community. And that's the largest single organization that reports to me. We also have a National Counterproliferation Center, a National Counterintelligence Center, and I really consider these operational, not staff units, because they were interagency groups that were doing a job, whether you had a DNI or not.

When you strip all of those away, you come down to the staff that has letterhead that says actual DNI on it. It's closer to 600. And to lead an organization of 100,000 is not – I think it's roughly right, and I'm adjusting it with a scalpel, not a meat axe. If you also compare it to the predecessor "Community Management" organization, which was housed at the CIA before the DNI was created, you'll find that when you add in the common services that were provided out of CIA – general counsel, public affairs, legislative affairs and all – it's probably about in line with what we had before.

So I think we're roughly right, but need some adjustment. The primary function that I find the DNI accomplishes that nobody else is doing is this drive on integration. And as I mentioned in my remarks, sometimes it happens naturally, but sometimes it needs a push from the top. I mean, everybody's busy; everybody's working on what's in their in-basket. When there's something that cuts across agencies, you've got to have somebody with a striped shirt and a whistle that says these are the rules. And I think that is the fundamental value that we add.

In terms of explaining that to Congress, I'm having very – the success that we all have in explaining things to Congress – some good days and some not-so-good days. But based on my experience, that's the way it looks. On the area of contractor support, I don't think there is a right number. We look at averages and what other comparable enterprises do. But the reality is that after 9/11, the tremendous growth of the Intelligence Community meant that all the jobs that we're given to do could not be done by federal employees.

We hired a lot of contractors from the mission; we had more money than we had people who could carry them out. Recently, we have one of the few in-government definitions of what an "inherently governmental function" is in the Intelligence Community. We actually sat down and wrote it down. Everybody knows the definition that a government worker ought to be – I mean,

there ought to be government workers doing inherently governmental work; but what that means has not been spelled out.

We've written it down in the Intelligence Community; and we are, in fact, in the process – and have been doing it this year – of converting substantial numbers of billets from, previously, contractors to government employees. And we're going to follow that template as we go forward. I think there's a strong place for contractors in the Intelligence Community, aside from things that we acquire – all of our big systems and our little systems are, in fact, built by private companies – but a role for contractors who are working in more direct-support roles, and many of the specialized functions that can be provided more efficiently there.

IT is a big one, of course. A lot of the common administration services, which are provided by contract to many private companies, can be provided to us just as well. That's an area. I also think that a lot of this flexibility for missions that happen for a while and may go away, are often better handled by contract personnel, because you don't know just how big the long-term corps is until you try it for a while. And of course, as you all know, many of the contractors who work for us are people with a lot of experience in the federal sector.

When I go in and talk to a team, whether it's in the ODNI or in CIA or other places, I have a hard time, unless I look at the color of the badge closely, knowing who is – you know, who gets a paycheck every two weeks and who gets it from a contractor. The mission dedication is the same; a lot of the knowledge is the same; the focus is the same.

So we get good teams there. So I think it's a program we're working through. I think we have a good plan in the Intelligence Community to be able to do it, and where the number shakes out is where the number shakes out. I think we ought to go from principles and let the number follow.

MS. BEAUCHESNE: I think we have time for one or two more questions.

DIRECTOR BLAIR: Okay.

MS. BEAUCHESNE: If you could get to the mic.

QUESTION: Could you tell us what the prospects are for long-term detention for some of the people you have held down at Guantanamo, how many and what the security assessment is if you bring them to the U.S.? And could you also tell us if you're considering rules beyond the Army Field Manual for your elite cadre of interrogators?

DIR. BLAIR: Those questions are the subject of a lot of hard work that's going on right now within the government and in consultations with the Congress. We in the Intelligence Community contribute a large group of our people to it. I was at a meeting yesterday; I've been talking with Congressmen and Senators about it in recent days. So I can't tell you right now where that's going to end up, but I can tell you that it's getting a tremendous amount of attention.

You may have read that the Justice Department announced a moving back of deadlines recently on a couple of key pieces of that group of issues that we're working. And although no one likes

to miss a deadline, looking at it from the inside, it's really a mark of the seriousness with which we are taking it, and of really taking the time to get the answer right.

MS. BEAUCHESNE: One more?

DIRECTOR BLAIR: Sure, I guess there are a couple in the back there. Yeah?

QUESTION: I wonder if you all have determined who was behind that July 4th weekend cyber-attack. Was it North Korea? And also, what steps is the government taking to prevent such things from happening in the future?

DIRECTOR BLAIR: The answer is that we have not figured out exactly who conducted that July 4th – that attack that began on July 4th. It was a relatively unsophisticated botnet-type attack, that nonetheless did deny service for some Web sites in this country. But the process of tracking it down is still going on. That is a good one – back to one of our previous questions – in which we're working with foreign partners to try to compare data to figure out if we can actually nail it down.

The reason that it's taking as long as it has is that, like most Internet attackers, the person who perpetrated this attack went through a series of cutouts – different IPs – and the process of going back and sorting that out just takes some time. And on that one, I am happy to say that the sorts of vulnerabilities in the system which made that possible were quickly passed around to others, so that they could make sure that their Internet was better-protected than that. I guess we have time for one last one, Ann, and then I'm on my way.

QUESTION: If I could ask you, earlier you spoke about building the relationship with Congress; how do you think the relationship with Congress has been affected in the wake of the killing of the program – the CIA secret assassin program, I guess you could call it? And do you support Director Panetta's decision to end that program, and why was there no notification given to Congress about the program up until late June?

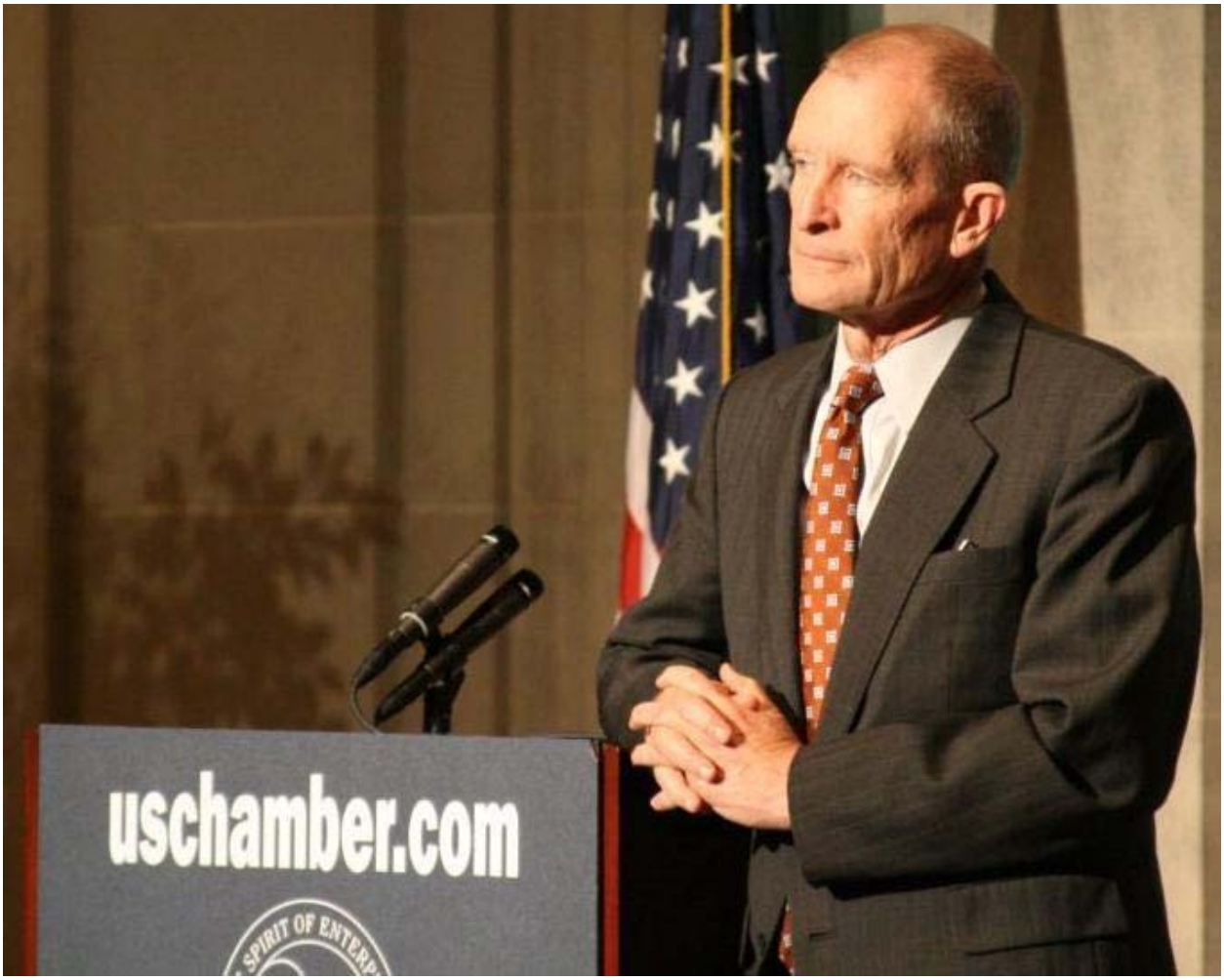
DIRECTOR BLAIR: What I'm finding in my six months in the job is that there are a lot of legacy issues that we have to work our way through, as we establish a new relationship with the Congress, and this is one of several. But I think what's really important is that we are working with the Congress in a new and I think better way. I find that I've been very clear with the Congress that we will lean on the side of telling them about things.

The statute says that we will inform Congress fully and currently of significant intelligence actions, and we take a very broad interpretation of that and tell them about – if there's any doubt in our mind, our default position is, let's tell the Congress about this. They're a partner in this. It's going to be better if we all work together. So what I'm really concentrating on, primarily, is making the new relationship going forward.

And we'll sort out these legacy issues, but I think that what most people want, and what we're really trying to do, is build this new relationship as we go forward, that we can work together as partners so we all make this country safer. Thanks very much, Ann. (Applause.)

MS. BEAUCHESNE: Thank you, Director Blair. Appreciate it. Thank you, everyone.

(END)



Director of National Intelligence Dennis C. Blair addresses the U.S. Chamber of Commerce National Security Task Force Meeting in Washington, DC on July 22, 2009.