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

The Commonwealth Club of California
San Francisco, CA

September 15, 2009

Related documents:

- Media Briefing by DNI Blair on the 2009 National Intelligence Strategy
- 2009 National Intelligence Strategy
- 2009 National Intelligence Strategy Fact Sheet
- 2009 National Intelligence Strategy Frequently Asked Questions
- Press Release on the 2009 National Intelligence Strategy

GLORIA DUFFY (The Commonwealth Club of California): Good evening and welcome to tonight's meeting of the Commonwealth Club of California. You can find us on the internet at commonwealthclub.org. I'm Gloria Duffy, President and CEO of the club, and I hold the gavel for this evening.

We very much appreciate the support of tonight's media sponsor, *The Wall Street Journal*, and an editor from the *Journal*, John Bussey, is here with us as our moderator for the evening.

At a time when the U.S. Intelligence Community has been both reforming itself to be smarter and more modern, and has been at the center of an emotional national and international debate about methods for obtaining information from terrorism suspects, we're delighted to welcome to our podium a man at the very center of these crucial issues.

Dennis Blair was appointed by President Barack Obama as the third U.S. Director of National Intelligence this past January, 29th. This is a relatively recently created position that supervises the heads of the 16 intelligence services of the U.S. government, including the CIA, the defense intelligence agencies, and the intelligence agencies within the Departments of Energy, State, Justice and other cabinet departments. He not only coordinates these agencies but serves as a Principal Intelligence Advisor to the President and the National Security Council.

A Rhodes Scholar and graduate of the U.S. Naval Academy, Adm. Blair is a sixth generation naval officer who has served in many theaters and positions, including commanding the carrier USS *Kitty Hawk* [Battle Group]. His naval field career culminated in his role as commander of the U.S. Pacific command or CINCPAC, as it is known, prior to his retirement in 2002.

Earlier in his career in the mid-1970s, Director Blair was a White House Fellow, and later Director of the Joint Staff at the Pentagon, the organization supporting the Joint Chiefs of Staff. His intelligence background includes serving as Associate Director of Central Intelligence for Military Support.

As Director of National Intelligence, Mr. Blair has continued the work of his predecessor in updating the methods and staffing of the Intelligence Community and making its activities as transparent as possible, given its mission. He's already made news prior to tonight's talk here at the club with a pre-release of his remarks in which he makes public some specifics about the Intelligence Community's budget.

Please give a hearty welcome to National Intelligence Director Dennis Blair.

(Applause.)

DIRECTOR BLAIR: Well, thanks very much, Dr. Duffy, for that introduction, and it is an honor to be invited to speak at this historic venue. Good evening to all of you.

Towards the end of my remarks, I'll give you some details on, as Dr. Duffy mentioned, what made news today. We released our National Intelligence Strategy, and there are even copies that I brought along that are available in the room, and there will be a pop quiz at the end of the evening. But after I've talked a little bit, I'd love to take your questions and turn this into a dialogue.

I've been familiar with the Commonwealth Club over the years – your lofty, ambitious mission: "To be the leading national forum open to all for the impartial discussion of public issues important to the membership, the community and the nation."

And when you add your motto: "Find the truth, and turn it loose in the world" – which I saw on the bulkhead as we came in – it's no wonder that you've been so influential, that you've developed such a fine reputation.

Most people think my motto is more like, "Steal the secrets, and make sure the world doesn't find out." (Laughter.) So I believe it's a mark of a truly open-minded group that you invited me, and I'd like to turn loose a little bit of truth about the world of intelligence this evening. So let's turn to a dictionary, and use it to help us sort through some of the irony and some of the contradictions in my business.

I think it's appropriate that I should use a dictionary that was compiled by a San Franciscan who disappeared in a foreign country almost a hundred years ago. What happened to him remains an international secret. It's eluded our best intelligence efforts since 1914. When he vanished, he was 71 years old – although he had a reputation as a tough old guy. At the beginning of the Civil War, he joined the Union Army as a teenager, served in the 9th Indiana Infantry Regiment, fought bravely on the Union side in battles like Shiloh, Chickamauga, and Kennesaw Mountain.

In 1886, his final stint in the Army, he'd by that time advanced to the rank of major, and he came to San Francisco. He liked it here so much, he hung up his uniform, began a career as a highly respected journalist, starting by publishing wartime experiences in several newspapers and magazines, including the *San Francisco Examiner*, worked for William Randolph Hearst, drank with Jack London, friends with Mark Twain and Bret Harte. You don't get more San Franciscan, I guess, than that.

And then in December of 1913, Ambrose Bierce went to Mexico for one last story – he was going to ride as an observer with Pancho Villa's army, and he never returned. He left behind many fine stories; but his most popular work, the one that everybody is familiar with, is the brilliant *Devil's Dictionary* – and on *The Wall Street Journal* today there was a sort of a picture of it in one of the inside pages, with a takeoff on some other definitions.

But Bierce's original work had typical entries like, "Diplomacy: The patriotic art of lying for one's country." And since your motto here at the Commonwealth Club of California is not lying, but finding the truth – I did some checking on some of those relevant definitions. I find, "Truthful: Dumb and illiterate." (Laughter.) That's not quite right.

Let's check some of the antonyms: "Fib: A lie that has not cut its teeth." Not helping. Let's try "Commonwealth: An administrative entity operated by an incalculable multitude of political parasites." (Laughter.) Even worse.

Now, irony and cynicism have their place. But I would like to counter some of the cynicism by removing some of the mystery that surrounds the intelligence business. It may be that we can't tell the public everything. But that doesn't mean that we can't let you know anything about who we are, and what it is we do.

In a republic, the intelligence services must have the trust of the public that they serve, and trust is not an entitlement – it's something you earn. So I can't tell you about all of the sensitive intelligence that we've collected today. But I can tell you that it's more than a billion individual pieces of data. I can't tell you the exact methods that we use to stop potential terrorists from coming into our country. But I can tell you that we have identified scores of people with previously undetected terrorist ties, long before they were able to reach our borders. And I can't tell you the methods we use to eavesdrop on suspected terrorists. But I can tell you if Americans or American telecommunications are involved, our actions take place or are authorized by a judge in accordance with laws passed by the Congress.

One way that I can talk about what we do in intelligence is to talk about some of the history, to bring some historical examples. And although some of the details have been updated, many of the essentials have not changed.

It was 59 years ago today – September 15, 1950 – that the United States landed on Inchon in Korea – one of the most daring and successful strategic military operations in world history. What you don't hear about Inchon is that a joint CIA and military reconnaissance intelligence team landed seven days ahead of time, and sent back essential information about enemy

fortifications and disposition, terrain, and tides. And they were key to what seemed at the time to be a miraculous operation.

Now, I've mentioned intelligence as a community. Curious word, but that's what we call ourselves: the Intelligence Community. And what is it exactly? Well, it's basically a commonwealth, but in the – I would say – non-Ambrose Biercian sense of the word. There are 16 organizations. As Dr. Duffy mentioned, we have separate agencies, we have bureaus that are inside other departments, and altogether about 100,000 people – military and civilian – get up in the morning and go to work in what we call the Intelligence Community, the IC.

And the larger organizations of the IC are fairly well-known. Dr. Duffy mentioned some of them: the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the National Geospatial Intelligence Agency, the National Reconnaissance Office, and the Federal Bureau of Investigation.

The CIA reports directly to me, and the other five are agencies in the Defense Department and in the Justice Department. And then there are ten more organizations that have substantial intelligence arms that are also part of this community.

The Drug Enforcement Administration falls underneath the Justice Department. Each of the services – Army, Navy, Air Force, Marine Corps – have large military intelligence components. The Coast Guard, which has an intelligence branch, is under the Department of Homeland Security, which has its own intelligence section as well. And finally, the Departments of State, Treasury and Energy each have an intelligence office.

And if you're counting, that's 16. And just that simple recitation of the number and where they're located will give you an indication of the complexity of the organization. They all have their own cultures. They all have their own proud traditions. And the trick, really – the mission that I have – is to bring them all together, so that we work together to do the right thing for the country. I'll talk a little bit about how we do that.

But one thing is, all the diversity means that there's a tremendous range of skills and expertise that we draw on to support policymakers, to support commanders in the field, to guard the safety of our citizens, and to protect the security of the country, which is our prime mission.

And my job was established shortly after the 9/11 Commission issued its 2004 report. One of the most important recommendations of that Commission was to integrate all of the intelligence elements in the governments. Five months later, Congress passed the Intelligence Reform and Terrorism Prevention Act. That act created the job I now have, Director of National Intelligence, when President Bush signed that into law in 2004.

Last November, I was surprised and honored to receive a phone call from President-elect Obama, asking me to join his team in this job. There ensued a serious family conversation with Diane, who finally agreed once again to postpone our retirement.

In my Navy career, I'd worked with the Intelligence Community a few times. As Dr. Duffy mentioned, I was the first Associate Director of Central Intelligence for Military Support back in the mid-'90s. And very early in my career, I was the intelligence officer on my first ship, which at that time was a collateral duty – an extra duty for a junior officer.

But most of my 30 years in my career, I was primarily a consumer of intelligence, and often, frankly, a pretty dissatisfied one. (Laughter.) So with a certain irony there, in being put back in this position. But throughout all that, I always had great admiration for those who collected the intelligence, those who analyzed it, those who tried to help the decision-makers and other officials do their jobs by telling them what our adversaries were doing and what they were thinking.

Any military commander can tell you that intelligence is extremely important to success. Some military commanders tell you there are only two outcomes for potential military operation: either operational success or intelligence failure – (laughter) – which is an indication of the importance of it.

But presidents, ambassadors, development workers, and law enforcement officials – well, I'll tell you that when they're supported by good intelligence, knowing what the environment is, knowing what's going on on the other side, the people that they're dealing with – they will do well, and it's that much better. And that really forms a core of what we do in intelligence.

In particular, I have three roles. The first role is as the principal advisor to the President on intelligence matters. If you consult "Advice" in *The Devil's Dictionary*, you'll find Advice is "The smallest current coin." I can assure you, intelligence advice plays, in fact, a large role in national security policy.

As a new administration comes in, it looks through the set of polices that it inherits to determine what it wants to do in these many important areas in the future; and I can tell you that in these seven months of this administration, the role of intelligence has played very strong as this administration has tried to figure out what's going on on the ground, what are the policies that got us to where we are, and what are the ones that we want to adapt for the future to support our interests.

In the Intelligence Community, we really go all out for the President, for the entire executive branch. They look to our support. I'm responsible for President Obama's daily intelligence briefing.

I also serve as the top intelligence advisor to the National Security Council itself, but that's only part of it. Intelligence officers, their reports, the whole collection system informs that entire national security policymaking process, which starts with interagency groups, works up through groups until it culminates in to National Security Council meetings and the President's decisions.

I also meet regularly with Congress, providing them with intelligence about what's going on in the world, and the status of our intelligence activities. If you look up the word "Senate" in

Ambrose Bierce's dictionary, he called them "A body of elderly gentlemen charged with high duties and misdemeanors." (Laughter.)

I can tell you that's not so for the two committees with which I deal the most often in the Congress – the Senate Select Committee on Intelligence, the SSCI, and the House Permanent Select Committee on Intelligence, the HPSCI. Their members are serious, dedicated patriots. And, in fact, some of the most prominent members of these committees hail from this area, and are clearly not elderly gentlemen.

Sen. Dianne Feinstein chairs the Senate Select Committee on Intelligence. I can tell you she's exactly the right person for that job – smart, tough but fair, always offering exceptionally thoughtful, critical, and useful guidance. She's just superb.

Rep. Anna Eshoo chairs the Intelligence Community Management Subcommittee of the House Intelligence Committee. Rep. Mike Thompson chairs the Terrorism/Human Intelligence, Analysis and Counterintelligence Subcommittee of the House Intelligence Committee. And both of them are excellent public servants who care about getting intelligence right. They're tough on us, but they're fair, and they have the nation's interests at heart.

And, of course, Speaker of the House Nancy Pelosi was the ranking minority member of the House Intelligence Committee before she became Minority Leader. And, of course, her experience with intelligence matters is now very important to all of us, now that she's the third highest ranking person in the government.

I can tell you they all represent you, San Franciscans, Californians well, and they keep me on my toes – as they should. They not only oversee all our activities, but they provide the budget for all of these agencies.

Now, this congressional oversight is crucially important in the area of intelligence, because so much of what we do is vital to our national security, but necessarily secret. And the intelligence committees have the appropriate security clearances. They represent the citizenry, so they're that indispensable outside check on all of our activities.

Turning to that important matter of money and the budget brings up my second responsibility as the Director of National Intelligence, and that is to manage the National Intelligence Program. The current year budget is always classified, but we publish the previous year's budget, which was $48 billion for National Intelligence Program.

And my job is to make sure that those resources are apportioned effectively across the Intelligence Community, to meet the major intelligence challenges that we're dealing with so – to get us a balanced program so that those 16 agencies can fulfill their proper roles in achieving the priorities that cut across all the individual organizations. We've just completed the process of justifying next year's budget to the Congress. And they looked at us hard, as they should.

Now, my third role is as the head of the 16-member Intelligence Community; and leading that community involves setting priorities, providing leadership on the cross-cutting issues that affect

more than one agency. And I try to align the incentives to enforce compliance, issuing policy directives that apply across the community. I clarify roles and responsibilities, and that's especially important for any activity that requires collaboration by multiple agencies. And the big, important issues all require collaboration by multiple agencies.

And then another important part of leading the Intelligence Community is to support the operations that we have in the field. Right now, we have diplomats, military units, reconstruction teams who are out there working in places like Iraq, Afghanistan, dozens of other nations around the world. And providing that support for all of these people out in the field is a key job of the Intelligence Community, and we do it extraordinarily well.

The sort of precise, tactical-level intelligence that we send out to those in the field is phenomenal. It's orders of magnitude better than the intel that I remember receiving as a junior officer in the fleet, and even what I saw as a combatant commander here in the Pacific about seven years ago. We try to give our units, our diplomats, our reconstruction workers an unfair advantage. They deserve it, and we're proud to provide it.

Now, underlying all of these three separate roles of the Director of National Intelligence is the fundamental responsibility to make sure that the Intelligence Community is coordinated, integrated, and is greater than the sum of its parts. We have to connect the dots better than ever before, to do all we can do to make sure there's never going to be another 9/11.

And, frankly, before 9/11, the general attitude of the Intelligence Community was to share information on a "need to know" basis. The 9/11 Commission concluded that the barriers to sharing intelligence were one of the factors that led to the failure – our failure to stop those attacks. So we've begun moving to a "responsibility to provide" mentality, rather than a "need to know."

And since the creation of this Office of the Director of National Intelligence, we've made tremendous progress in sharing information. That's not only true within those 16 agencies I talked about, but also with other partners that we have in the United States – the Department of Homeland Security, law enforcement officials at the local, state, tribal levels. And we've worked hard to improve the necessary communications with our foreign allies, and with those in the private sector.

Now, sharing doesn't come naturally to us spies, but it's got to change. We recognize it does; and, in fact, it is changing.

As we go about this reformation of the – and improvement of our intelligence business, one of our big advantages, and at the same time one of our biggest challenges that we have – and I'm guessing this is of particular interest here just up the road from Silicon Valley – is the growth of information technology.

For our intelligence analysts, it raises real challenges to sort through terabytes of intelligence, or even petabytes of it – I didn't even know what a "petabyte" was until a few years ago, but we've got them – they have to – these analysts have to – sort through all of this huge mass of

information to spot trends, to find out what's correct, to find the invaluable individual pieces of information that are in that mass of data that comes into it.

And many of the tools of the information technology revolution have helped us in that sorting process and in the sharing process. But these added tools – the opportunities, the unprecedented volume – also bring a host of vulnerabilities, both for the Intelligence Community and for the country.

Three Presidents now have declared that our cyber infrastructure is a strategic national asset. And protecting that asset is a high national priority. The threat to that infrastructure comes from nation-states. It also comes from hostile, non-national organizations, and even from skilled individuals.

And our cyber infrastructure is intertwined – the systems we use for intelligence, other national security functions, other government networks and private systems use many of the same cables, many of the same service providers, many of the same switches and the same applications.

Now, the United States is not vulnerable to cyber attack to the degree that countries you may have read about like Georgia and Estonia, which have been attacked in recent years. Our infrastructure is so big, so complex, that it doesn't have that sort of vulnerability. And in addition, we get a lot of practice all the time dealing with both attacks, hackers and with natural problems which force people to learn their systems and to make improvements.

But to keep those networks safe, we have to continually improve these systems, improve our skills, improve our defenses, as the hackers develop new attacks. And at the same time, we need to share ideas and best practices, so that American businesses can protect their private networks, which are also increasingly at risk from these same techniques. And they have to help us. We must take advantage of Silicon Valley's vast expertise – that constant innovation that comes.

It's the Department of Homeland Security that has the lead role to protect both the government and private critical infrastructure on which our national life depends. One of the most important agencies working with the Department of Homeland Security is an intelligence organization, the National Security Agency. It has an unmatched understanding of computer networks.

The NSA's technical capabilities and their expertise are absolutely critical to protecting our digital infrastructure. But the idea of using NSA's technical capabilities to help protect networks in our country often causes concern among some citizens. We must and we do use our capabilities in a way that assures our citizens that their privacy and their civil liberties are protected.

Americans must and they can have confidence that the technical capabilities of the Intelligence Community are being used to save lives and protect our nation, that they aren't being used to warehouse private information about Americans. We must and we can do our job under the oversight of the Congress and overseen by the courts.

So I believe that the Intelligence Community has a huge responsibility to help protect federal networks, to warn about the threats that are there, to share techniques that we've developed, and that we can do it without intruding on the civil liberties and the privacy of Americans. We have to continue to cooperate with those in the private sector on whose networks much of the critical infrastructure resides. And we have to do those jobs carefully, under supervision, entirely within the provisions of the law, with proper oversight from both the legislative and the judicial branches.

Let me brag some on those 100,000 men and women of the Intelligence Community. They're smart, they're dedicated. I'm just tremendously proud of them. More than ever, we need employees from all backgrounds, all races, all cultures and all religions, because we need as diverse a workforce as the world it is that we're trying to understand.

If you look the numbers in recent years, we've done better on that line. We're not where we want to be, but we're getting closer all the time. And we recruit more than the brave men and women who go out on the dusty streets to gain information in hostile countries. We also need and have linguists, criminal justice experts, lawyers, economists, researchers, historians, political scientists, cyber-security specialists. We have engineers who work on advanced satellites, communications equipment, sophisticated sensors, facial recognition technology; and analysts who can make sense of that flood of data that we receive every day. That's your Intelligence Community.

The Partnership for Public Service recently selected the Intelligence Community as one of the best places to work in the federal government. I think it's especially remarkable – but not so much – when you realize that half of our workforce has joined since 9/11. Half of those 100,000 who work in the Intelligence Community signed up after the World Trade Towers and the Pentagon attacks. So they're a group who's been inspired by the patriotism that flowed from that event – and which has always been a part of this country's heritage.

Turning to *The Devil's Dictionary* again: "Patriotism: In Dr. Johnson's famous dictionary, patriotism is defined as the last resort of a scoundrel. With all due respect to an enlightened but inferior lexicographer, I beg to submit that it is the first." (Laughter.) Again, it's fun to be cynical sometimes, but I just couldn't disagree more with that definition.

In the Intelligence Community, we don't have loud, boisterous, flag-waving types. We have quiet professionals who care about what they do. They know we can't give them much public recognition and their reward is really contributing to a safe America.

Now, those who serve our communities, and on occasion have to go in harm's way, have a special respect from their fellow citizens: the armed forces – soldiers, sailors, airmen, Marines, and Coast Guardsmen who serve this country proudly. The police officers who keep our streets safe – federal, state, local. And of course, the firefighters and first responders – I'm sure that those of you who live in a state where deadly wildfires are a recurring event, that experienced the World Series Earthquake of '89, the Great Quake of 1906 – a city that sponsors Fleet Week every year – are mindful of and are thankful for those who serve us on a daily basis.

But I would like to tell you about another group of professionals who protect their fellow citizens, who put themselves into harm's way; but who typically do it in secret, receiving little public recognition – and those are members of this Intelligence Community I've been talking about.

They're sometimes even viewed with suspicion by their fellow Americans. But like the armed forces, the police, firefighters, first responders, we too have lost people in the line of duty.

The Central Intelligence Agency has a Memorial Wall with stars carved on marble to represent those killed in action. Some of their stories still can't be told today but others can, like the first CIA employee killed back in 1949, Douglas Mackiernan. His service was finally acknowledged in 2000 in a ceremony with his family – that was a closed ceremony – and finally made it public three years ago after [nearly] 50 years had passed. In 1949 at the end of the Chinese Civil War, when the communists established the People's Republic of China, Douglas Mackiernan stayed behind in the deserts of Western China to destroy some sensitive equipment and to help some anti-communist leaders. He made it out, survived the Taklimakan Desert, the Himalayas, went on his way to India; but was mistakenly shot and killed by Tibetan border guards as he entered across the border.

The National Security Agency also has a Memorial Wall that has even more names than the CIA. The Military Intelligence Corps has, of course, lost many members of the different armed forces. The FBI lost intelligence agents as far back as World War II.

The Defense Intelligence Agency has its own Patriots' Memorial. One of the saddest stories there was in 1975, when five DIA employees stationed in Vietnam were helping take care of 250 orphans being evacuated, when their Air Force C5A crashed on takeoff from Saigon. Seven more DIA employees were killed on 9/11 in their offices in the Pentagon. And just last week, four more were wounded in Afghanistan.

It's a dangerous business. But the people who do it do it gladly, they're proud to serve. They're proud of their country.

The Devil's Dictionary defines "Valor" as "A soldierly compound of vanity, duty and the gambler's last hope." But I can tell you as I continue to review and approve the awards for the Intelligence Community, vanity has nothing to do with it. These individuals are truly inspirational. It's enough to eliminate the cynic in anyone to read those citations, and to get to shake their hands.

And I hope that over time, we can make Americans just as proud of their Intelligence Community as they are – and rightly so – of those who serve in the armed forces, law enforcement, first responders.

So what about the future for this Intelligence Community?

Ambrose Bierce defined the "Past" as "The region of sobs," and the "Future" as "The realm of song." And for once, I agree at least in part with his definition, because I am quite optimistic about the future of the Intelligence Community.

As I mentioned, earlier today, my office released the National Intelligence Strategy. And so today is the first time I've really had to talk about it in a public forum. It gives us our marching orders – our blueprint for the next four years. We wrote it and extensively coordinated it with the members of our 16 organizations in our Intelligence Community, also with the National Security Council.

And it contains four strategic goals. The first is to enable wise national security policies. We plan to do that by continually monitoring and assessing the international security environment, so we can warn policymakers about threats that are out there, and we can also alert them to opportunities.

Our second strategic goal is to support effective national security action. I talked a little bit about this – to deliver "actionable intelligence" that supports diplomats, military units, interagency organizations in the field, domestic law enforcement organizations.

Our third goal is to deliver balance and improving capabilities so that the future Intelligence Community can be even more effective than that of today. We have to stay on the cutting edge of technology.

And our fourth strategic goal is to operate as a single integrated team. If there's one thing I'm positive about after my short time on the job, it's that we're far more effective when we work together as a team, when we share information and skills, work closely with policymakers or with units in the field.

The strategy goes on to lay out our mission objectives; that is, what we intend to accomplish: tasks like combating violent extremism, countering weapons of mass destruction proliferation, and enhancing cyber security. And it also lays out our enterprise objectives, or how we'll get the job done: improved integration and sharing, and improved acquisition.

And the strategy calls on us to be more agile, more integrated, and to exemplify American values.

Agile because threats and opportunities in today's world come quickly and they go quickly, and you've got to catch them when they're there.

Integration – I told you I've seen firsthand how the Intelligence Community produces amazing results. I wish I could take you into a darkened room with a flickering computer screen, and seated at that computer screen is a young sergeant, Army, Air Force, male, female sitting in uniform on the keys, looking at a screen which is inside a computer halfway around the world of somebody we're trying to get some information about, or are trying to make him do something or stop doing something. Over here is some young guy with a New York Yankees – generally haven't got a San Francisco Giants baseball cap – it's on sideways, little goatee. He's saying,

"Hey, you're doing well. You're getting in there. Stop right there, move back a little bit. You got them." On the other side is the young woman who speaks the dialect of the country that we're – this computer that you're working on, and she's working with the young sergeant to make sure – understand the nuance of what's on that screen, how you can move, what you need to do.

Usually, in the back there's some grizzled old person about my age who's been doing signals intelligence for 40 years, who sort of has the overall picture of what's going on there; and then three or four other people in the back who've been working on that same problem that are helping in this team with the computer we're trying to work half way around the world.

It's something that happens every day. When it happens together like that – as a team, bringing all the skills that we have together – real, real magic happens.

And welding teams like that together – whether it's what I can do by what I do at the top of the organization, or through encouraging this sort of idea, nourishing it from the bottom up – that's how we really achieve the best results for this country in the intelligence world.

Our world is a world of secrets, but it need not be, as I said, a world of mystery. Our people join for patriotic motives. Their jobs are about protecting the lives and security of Americans. I want them to be proud of what they do; and I want you, the American public, to be proud of them also.

So aside from what's in the National Intelligence Strategy, let me emphasize what I think is the real news here, which is that our Intelligence Community is as transparent as possible to the American public. We do have to protect sensitive sources and methods, but we've actually published our National Intelligence Strategy for all to read. Our enemies can read it, but we mainly publish it for the American people. You can have a copy tonight as a souvenir.

Why do we do that? Because we believe that if the public understands a little bit more about what we do and why we do it, overall we'll be a stronger, safer nation for it – one with confidence that we in the intelligence business are doing the right thing for the country.

As we often do in this great country, we're conducting an amazing experiment in democracy – a magnificent experiment. Can we operate a large, powerful, effective intelligence enterprise while adhering to the American principles of openness, separation of powers, respect for privacy? I believe we can do it. And so let me close with this.

U.S. intelligence existed back in 1913 when Ambrose Bierce disappeared, although at that time, there was Army intelligence and Navy intelligence, and they didn't talk to each other. But even so, if they had talked to him, I bet their assessment to him would have been – had he asked: Not the smartest thing to go down as an "Old Gringo" at 71, to go palling around with Pancho Villa in the middle of the Mexican Revolution.

Maybe he went out more of a legend that way – the extra mystery surrounding his disappearance. But personally, I wish he'd come back to the United States, to write at least one more story.

And that really brings us to today's Intelligence Community. We want to keep Americans safe so they can keep writing their stories: so they can keep running their businesses, so they can be secure – as they have dinner with their families, see the Giants and the A's, the Forty-Niners, the Raiders play ball, go sailing and fishing, drive up and down the Pacific Coast Highway, take care of each other, educate their kids, go about their civic duties. So they can live the American dream. That's our responsibility – is trying to make that life as safe as possible. We take it seriously, and I think we can do it right.

So let's turn from a monologue into a dialogue. There's a lot we can talk about. I'd love to hear your questions and your ideas.

And thank you very much.

(Applause.)

MR. JOHN BUSSEY (*The Wall Street Journal*): Well, thanks very much to Director Dennis Blair, the Director of the U.S. National Intelligence Directorate (sic). The range of questions I've received – some of you I'm going to come find after this meeting and hire you for *The Wall Street Journal*. These are terrific questions and they sort of range across zones like cyber security, lessons learned from 9/11 and Iraq, to how to wrangle the sort of far flung bureaucracy in Washington sort of into some effective sort of fighting vehicle. And then at the end of all these questions, and this will be for the last one to keep you here until seven o'clock, "did you really water-ski behind the *Kitty Hawk*," which is something I'm very curious about as well. (Laughter.)

Last question, first. The notion of this vast bureaucracy in Washington, all of these different intelligence agencies, one questioner said, shouldn't we just merge some of these? Isn't it just inefficient to have them – have so many of them? They've kind of grown up of their – sort of in their own directions and never been pulled together. What challenges do you encounter with the culture of the various agencies you have to coordinate? Are there still silos and separation of information? Can we now connect all the dots, or will we be playing Monday morning quarterback again? And I think that one question that summed up this topic for us and maybe you can tackle all of them at the same time: Had the organization that you had now been in place pre-9/11, do you think the 9/11 attacks would have occurred?

DIRECTOR BLAIR: The serious consideration of this question about how we organize the intelligence communities was done as a result of that 9/11 Commission and within the commission itself, and then in the subsequent congressional consideration of the debate. That range of possibilities for organizing intelligence was considered. On the one hand, create a Department of Intelligence, put all of these 100,000 people and $50 billion budget and put it in one department, and then that Department of Intelligence has a job then of providing it to everybody who needs it.

And it was decided not to form that separate department, but to form more of a confederation, and to give to the Office of the Director of National Intelligence certain key authorities: budget, setting the rules for sharing of information, personnel authorities. And the reason that was done

that way is because intelligence is such an integral part of what many organizations do that the idea of ripping their own intelligence arms out of that department, whether it be Defense or Treasury or DEA, would destroy the real responsiveness of the intelligence. Better to be leave them there working with other intelligence agencies and making the whole work.

So that was the basis of decision. And from what I've seen, that was a good solid decision. But it does put a premium on trying to work against your departmental demands sometimes, and for the greater good and the working together. And the way we do that is to try to concentrate on the definition of the task, the mission. Example: What are the leadership intentions of country X? Go steal the secrets, do the analysis to find that out, because a lot of people need to know about it.

Example: Country X is developing a weapon system that could be used against Americans. Go find out what its characteristics are, so we can build counters to it.

Narcotics gang Y is out running drugs across international borders. Find out about what they're doing, and tell that to the people whose job is to go stop them and arrest them.

So when you try to organize by mission, bring the team together from these different organizations, that's when the good stuff happens. So I think if we leave the agencies in these current departments, we give them a mission. We give somebody like me the authority to make sure that their budgets cover those things, that they can share information, and that they're well plugged in with the people who need the information. Then we can make the right things happen in the right way.

So so far I think that's the right way to do it. And yes, if we'd had this organization, if we'd had this system of working back on 9/11, I don't think that the attacks would have occurred. We now know enough about many of these terrorist organizations that wish us harm that we're stopping them with far less information than was available back on 9/11/2001. So I think that we are doing a better job than we were then; and had we been in existence back then, we would have stopped them.

MR. BUSSEY: I think the intent of that question was probably to ask whether or not these different bureaucracies do in fact share information. And Mike McConnell, the previous DNI – one of his bits of advice to you was that this needs to be constantly improved.

Is there something that you can tell us that is not classified that illustrates how information is now being shared between these agencies in a productive way, where it had not been shared before?

DIRECTOR BLAIR: I can give you a good example based on the systems that we're deploying to Afghanistan now to support the diplomatic, economic reconstruction, military effort that we have there. In order to do this integrated job in Afghanistan – which is work with the Afghan national security services, work with Afghan government, provide security, bring a certain amount of governance, and then provide some economic assistance – we have created an information system on a network housed in computers accessible at various levels of

classification by nongovernmental organization, accessible by allies who are working with us there, accessible by USAID workers, accessible by U.S. military officers. And it's all in that same database in which you can find the latest attacks that have occurred in the region where you are. You can find the identity of village leaders. You can find out what the crops in the fields are. You can look at pictures which have geospatial information with the map. So that kind of getting everybody to contribute to that same database and then having accessible by all the people to use it, I think is probably one of the most developed examples of what happens now.

MR. BUSSEY: That relates to another question we got. It's kind of similar to – and Afghanistan may be a good example of this. Can you describe the type of information the battlefield soldier now has at his or her disposal compared to the past and the technology they use to access it?

DIRECTOR BLAIR: I'd say the primary – to think about in the past, the information that we would obtain from our very best systems, we would limit the distribution to certain elite units. This was true as recently as Iraq. We found ways to strip out the sources and methods of that information, so we can make it available to any soldier on a geographic basis in the area in which he or she is operating and make it available to others. So it's that ability to take what was previously highly classified, very limited distribution information, and make it available to everybody who needs it, that has I think made a real difference on the tactical front now.

And we certainly didn't have it when I was growing up in the armed forces. That was a secret stuff that you had go back into some room to read, and then you had to destroy it after you read it. You had to try to remember it. You couldn't take notes. Now we put that information out where people can use it where they need it, and it's made all the difference.

MR. BUSSEY: Some cyber security questions and internet questions. Hackers – any place in the world, they're breaking into protected networks, even apparently the Pentagon. Can you assure us of the safety of our secure networks and systems? And this one: The U.S. economy seems ever more reliant upon the internet for daily commerce. Do you see mounting evidence of a potential attack on or through electronic infrastructure, and from where?

DIRECTOR BLAIR: I don't think – from what I've learned about cyber offense and cyber defense, and the advantage of having the Intelligence Community involved in this business is that we're the ones who go out and use these techniques to steal other people's secrets, so we know what can be used against us, and that can inform our defenses in a very good way. And what I've learned in this business is that there's no final answer. The offense learns something. There's a hacking attack that's discovered, throw up defenses. Offense goes out to another attack, and it's one of those games of offense and defense – a crew race, who's taking the last stroke.

So that means that you can't rely on some solution. We can't go down and tell somebody, "Give us the ultimate firewall. Give us the ultimate safeguard." What we have to rely on is the skill and ingenuity and the hard work of our cyber workers, compared to the people who are trying to come after us.

So we try to set up a system so that the things that we know are threats, we can build the defenses to, and we can put them up as fast as the threats come at us. And some of the attacks that have been talked about publicly coming against government systems, we – our more secure systems are protected by more layers – and we keep those okay. But the systems right next to the internet – the dot-gov network, which we rely on both in all the branches, certainly the dot-com network on which power grids of electrical companies, banks, tunnel through those for their business – they're right up close to the internet where anybody can roam, so we have to keep improving the defenses, detecting attacks, and knocking them out.

So it's really a continuous game, and I would say that overall we're staying ahead; but it takes an awful lot of hard work to do it.

MR. BUSSEY: This is just for our radio audience. You're listening to the Commonwealth Club of California radio program and our speaker today is Dennis Blair, who's the Director of U.S. National Intelligence.

Back on this question of cyber security, though, this seems to be an increasingly large focus of our Intelligence Community. And I wonder if you could answer that part of the question that asked where is this coming from? And is it coming from a country that has state involvement in it or is it coming from criminal groups? What is the kind of the primary cyber threat now to the United States?

DIRECTOR BLAIR: If you count them up, most of the attacks against American cyber systems originate in the United States – sheer volume. Not all of those originate, because as many of you know, you go from one computer to another in order to attempt to disguise, and the final IP from which you make your attack on a circuit will generally be several hops from where you were. When you trace it all back, we find a huge amount of activity coming out of China. We find a lot of activity coming out of Russia. We find a mixture there of unofficial and semiofficial backgrounds. But that attribution is a tough part of the cybersecurity business, so we don't have as much certainty as we'd like to as to exactly who's behind the attack. But those are the countries that a great number of them come from.

MR. BUSSEY: We have people participating on the Internet as well. This is a question from one of our Internet participants. How do you and other senior officials of the Intelligence Community plan to assure that there are no further abuses of detainees in the custody of U.S. intelligence agencies?

DIRECTOR BLAIR: Because we're not going to have any detainees in the custody of the U.S. intelligence agencies. (Laughter.)

MR. BUSSEY: Really?

DIRECTOR BLAIR: Yes. You'll be talking with Director Panetta here shortly as you mentioned. We have closed down all of the facilities that we had for the Intelligence Community detaining personnel that we can get overseas. All of them who we may detain in the future will be taken care of in some sort of national facility which will be – we're deciding who's

going to run it, who's going to run it now, but there won't be any from the Intelligence Community. There won't be any run by intelligence agencies.

Another controversial part was the questioning of detainees, and we decided that going forward for the high-value detainees, we're putting together an interagency interrogation system that will have – it will take the best intelligence analysts, Department of Defense, FBI, interrogators and supporters; and we'll put together one team whose job it is to interrogate those high-value terrorists that we are able to catch in the future. So that's the new system going forward. We still have to deal with the 200-some-odd detainees who are in Guantanamo Bay. A lot of work is going on on that right now.

MR. BUSSEY: We have a couple of Pelosi questions as well. No surprise. Other than Mrs. Pelosi, has anyone in government ever accused the CIA of not being truthful with Congress? Your thoughts on her charge, please. (Laughter.)

DIRECTOR BLAIR: Nice question. I think the – one thing I did notice, and Leon Panetta noticed when he came into – when we both came in here about seven months ago, was that the relations between Congress and the Intelligence Community were just under tremendous strain. And we've worked tremendously hard to put them back where they ought to be – as more of a partnership, rather than a complete adversarial relationship.

So let me speak for the future. We don't lie. We tell the truth and nothing but the truth. We just don't tell the whole truth. (Laughter.) And to the members of Congress – that's in public – to the members of Congress who have the clearances, we tell the truth, the whole truth and nothing but the truth. We tell them what we're doing. They have the clearances to know it. They should know. They should be informed. And so that's what we're trying to do moving forward.

MR. BUSSEY: Can you talk to us a little bit more about that relationship with the CIA? Here's an institution that had cut its own course in Washington for decades. What's your relationship like with Leon Panetta now that you're structurally his boss? And how much do you talk to him? And how much guidance do you give the CIA? And how much do you just say that that's an institution that knows its mission and your attention is elsewhere?

DIRECTOR BLAIR: I talk with Leon all the time. We're constantly working on the same issues. Within this community that I described, the CIA has a couple of missions. They are in charge of human intelligence. They are the ones who go out and recruit spies. And they're also in charge of leading that organization for all the intelligence agencies that are in the human intelligence business. And we do that in many, many other agencies. They also have a large group of so-called "all-source analysts," so the different types of intelligence that we draw from signals intelligence, human intelligence, geospatial intelligence, comes in, and in many, many cases it's Central Intelligence Agency analysts who are the ones who put it together.

In addition, the CIA has the job in nine cases out of 10 for conducting covert actions – actions that we wish to take from the Intelligence Community to support international – to support our national goals. So those three goals within the – that's what the Central Intelligence Agency carries out, and Director Panetta is responsible to the President and me to do those. My

responsibility is to put those pieces together with the other agencies to get the job done and these teams that I talked about.

Previously, his job and mine were together. The Director of Central Intelligence was also the Director of the Central Intelligence Agency; and when you talked to – when I talk to my predecessors who've had both jobs, they told me that there was plenty of work there to split it into jobs for two people – trying to lead the community and to run the CIA; and I agree with that.

MR. BUSSEY: Your views, please, on the NSA's domestic telephone surveillance program.

DIRECTOR BLAIR: As I said in my remarks, the job of the National Security Agency is to gather foreign intelligence. When foreign intelligence leads us to conduct operations that may involve an American or may involve information located in the United States, we go to a judge, we get permission, and then we have to conduct it under those strict guidelines, both the way information is collected and the way it's passed around the community to use, to build this total picture all under the guidance of the FISA Court. So that's basically how we did it, and how we have done it ever since the legislation was passed in 2005 (sic).

MR. BUSSEY: I have a budget question for you. The writer takes note of the large budget increase that you announced today, $75 billion, I think up from roughly $40-$45 billion earlier. One question from the writer of this: Where is that going to be spent? Is it the bulk of it headed toward Iran, North Korea, China? What activities? Are they external or homegrown? And then, just so – my question: Is that money that has always been in the Intelligence Community's budget, but is now just being made public?

DIRECTOR BLAIR: I need to make the figures clear. The budget that I mentioned in my remarks earlier, the National Intelligence Program, which last year was $48 billion, that is the money that is spread among those 16 agencies. And as I mentioned, we announced the total figure for the past year just so people have an idea of roughly how much we're talking about. We don't publish – nor am I going to make news tonight telling you how much each individual agency is funded for and what it's used for.

This morning, in answer to a question of what is the total effort for the Intelligence Community, I mentioned the figure $75 billion, and that includes not only the $48 billion in my program, but roughly half again as much which is in other activities which are related to the budget which goes for the purposes of intelligence. Those are two different figures. And I think that's about all I'm going to tell you about the money. (Laughter.)

MR. BUSSEY: A simple question from one writer. What keeps you up at night?

DIRECTOR BLAIR: It's the – it's worrying about whether we've done everything we can to stop the terrorist groups that seem to think it's a great idea to kill a lot of Americans. We know a heck of a lot more about that than we did before. We can be a lot more aggressive in going after their organizations than we could previously. But in today's world, when it takes so few people, so little equipment, and so few scruples to cause a lot of damage in this country, you just worry that you – you worry that you haven't done it all. So that's the main thing.

MR. BUSSEY: Many departments in the federal government will be facing large numbers of Baby Boomer retirements. How do you effectively recruit the next generation for service to the country? And I wonder if maybe we can turn that question slightly. There's been a very large recruitment of intelligence analysts since 9/11, and I wonder if the type of individual that you are recruiting now – younger, Internet savvy, Facebook, MySpace, used to sharing information – is helping you in the goal of interagency information sharing? So one question is: How are you going to replace all these people with qualified individuals? And the other: Is the nature of the individual who's coming into the departments a different sort of cat?

DIRECTOR BLAIR: Right. The demographic profile of those hundred thousand people in the Intelligence Community that I mentioned is sort of dumbbell-shaped or nut-shaped. We do – 50 percent of them, as I mentioned, came in since 9/11, so we have a lot of fairly new, not all of them young, but new to the intelligence business. And then we have those of us who were sort of the Cold War generation going out. So I think as that new generation works its way through and gains more experience, that will be good. And working with them – I gave you a little bit of description: incredibly hard working, savvy – it takes a little bit of adjusting. We have a classified MySpace network that we use to get analysts together to talk about things. And I bet on any given day I'll open my e-mail and say, hey, Dennis, I'd like to be your friend. So I write back and say I'd like to be your friend too.

MR. BUSSEY: That was Kim Jong-il, by the way, saying that one. (Laughter.)

DIRECTOR BLAIR: So it's an organization that I think is more flexible. And I think the – what I find is that the further you get from Washington, the younger you get among intelligence officers; the more they have this idea of team/mission/results. So I'm very optimistic that when one of them is sitting up talking to the Commonwealth Club here in 30 years, it will be an even better organization.

MR. BUSSEY: What percentage of your time is spent dealing with terrorism? And then, after terrorism, what is the next most important national security matter on your list?

DIRECTOR BLAIR: Our two top sort of overarching threats are violent extremism – people want to come kill a lot of Americans – and countering the proliferation of weapons of mass destruction. So those are the two that we are spending the most time on, as real crosscutting challenges to us. Some of those come together in individual countries. In the case of Iran, of course, it's their possible nuclear weapons program that is of most concerns, so it cuts across the country. The issues of terrorism, of course, blend with the traditional national concerns about the countries from which terrorism comes: Pakistan, Afghanistan, elsewhere in the Middle East. So it's that really nexus of these crosscutting issues and individual countries; that's really where we spend most of our time.

MR. BUSSEY: We have a question along those lines about proliferation. One of the goals of the National Intelligence Strategy is countering weapons of mass destruction proliferation. What gaps do you see in our current capabilities to counter proliferation, and how would you see bridging those gaps, weaknesses in our system?

DIRECTOR BLAIR: We have a good system with a lot of emphasis on that, but it's hard work. Countries and especially other organizations that are trying to develop nuclear, chemical, other programs want to hide them. They're fairly good at hiding them. When we're dealing with countries like North Korea – which recently announced that it has a uranium enrichment program in addition to the plutonium program that it accomplished, or that has previously acknowledged – [that] gives you an idea of the complexity of what we're up against. There's the shadowy netherworld of arms dealers. The A.Q. Khan network coming out of Pakistan was the worst of these in recent years. And here was an organization that built national nuclear weapons in Pakistan, and then decided to go out and sell the technology to a bunch of other countries, and wanted to hide it while it was doing it.

So it's the sheer difficulty of the – it's the sheer measures that people are taking to hide it that makes it the most difficult. In addition to having a very strong human component, who are the people are who are doing it, trying to learn about them; the technical component, just what is the actual possibilities that a country has a weapon, that it's gained the combination of technology and people. So it just makes it a very, very hard problem.

MR. BUSSEY: Are the Russians and the Chinese in your mind partners in that effort, or do they see allowing an Iranian nuclear program, allowing proliferation out of North Korea, as an opportunity to keep the U.S. a little off balance?

DIRECTOR BLAIR: The Chinese and the Russians don't like nuclear proliferation any better than we do. They generally feel that it makes it a more dangerous world. There's sometimes a difference in the degree in which they are willing to work with us, and put both pressure and inducements out to other countries, because they have other interests with them. So I don't think there's any difference on the foundational goal of trying to reduce and counter proliferation. There's sometimes less urgency, less willing to put it at the top of the priority list with Russia and China.

MR. BUSSEY: North Koreans found building a nuke plant in Syria, boats shipping out of a port in North Korea headed toward Myanmar – those aren't things that China could put the kibosh on, if it wanted to turn off energy and turn off food to North Korea?

DIRECTOR BLAIR: China was helpful to us with the *Kang Nam 1*, the North Korean ship that was going to Burma. That was a good international effort. I don't think I'll comment a lot about the Syrian program. That's still pretty classified.

MR. BUSSEY: Okay. We have room for one last question before the time is up and so maybe you would comment on this. Is this just a wild rumor, or did you really water-ski behind the *Kitty Hawk*?

DIRECTOR BLAIR: No. It's correct that I tried. It's incorrect that I succeeded. (Laughter.)

MR. BUSSEY: It's a very large propeller. I'm very glad that you're here with us today.

Our thanks to Admiral Dennis Blair, Director of U.S. National Intelligence. We also thank our audience here and on radio, television, and the Internet. The media sponsor today is my publication, *The Wall Street Journal*. I'm John Bussey with the *Journal*. Thanks very much for coming here tonight to the Commonwealth Club.

(Applause.)

(END)