Center for Strategic and International Studies (CSIS)

“The Evolving Terrorist Threat and the Importance of Intelligence to Protect the Homeland”

Intelligence to Protect the Homeland and the Way Ahead

Speaker:
John Brennan,
Assistant to the President for Homeland Security and Counterterrorism

Moderator:
Fran Townsend,
Chairwoman,
INSA

Wednesday, September 7, 2011
11:00 a.m.
Washington, D.C.

Transcript by
Federal News Service
Washington, D.C.
FRAN TOWNSEND: Hi, everybody. I thought before we started – John, I thought it was appropriate – in my office, when I was in that office in the White House, I hung this flag of honor, which has the names of all of the victims of the 9/11 attacks, and I thought it would be appropriate to hang it today for the conversation.

JOHN BRENNAN: That’s very nice.

MS. TOWNSEND: Ladies and gentlemen, John Brennan is a friend, a colleague, a patriot and an enormously talented individual. He was appointed as assistant to the president for homeland security and counterterrorism in January of 2009. He is a 25-year veteran of the CIA, having held several key overseas positions, particularly in the Middle East, that provide him a unique perspective regarding current conflicts and challenges.

He was instrumental in the establishment of the Terrorism Threat Integration Center in 2003 and managed its transition to the National Counterterrorism Center that it is today.

Upon leaving government service in 2005, John formed his own successful company and also served as the chairman of INSA from 2007 to 2008. And I sort of like to say we did a job swap. I came out of government. I became chairwoman; he went into government.

We are fortunate to have John with us today to talk a bit about the threat to the homeland from his perspective and the way ahead with regard to protecting our homeland.

John, why don’t you start?

MR. BRENNAN: You ready to swap jobs again, back now?

MS. TOWNSEND: No. (Laughter.)

MR. BRENNAN: Well, thank you very much, Fran, for inviting me here. And thank you to INSA and to CSIS for sponsoring this event, which I think is very important. It’s nice just coming in here and looking out on the audience and seeing so many familiar faces and so many of those faces that I worked with 10 years ago and since then. And I was mentioning that it seems like in many respects yesterday, but in other respects it seems like a lifetime ago, that tragedy on 9/11.

This week, I think, is a week for remembrance of the victims, as well as just taking stock of where we’ve come over the last decade. I had the opportunity to meet with several members of the 9/11 commission earlier this week when they issued their report card about the types of
things that they think that we have done well and other things that have not been followed up on in terms of recommendations.

And I was just talking with Judy Woodruff for the “NewsHour” and commenting that, you know, we really have, I think, done an impressive job as a country over the last decade, both in terms of the threats that we face from overseas and mitigating that threat but also making the United States a much less hospitable environment for the terrorists to operate. We’ve been able to identify vulnerabilities and take steps to, you know, fill those gaps that are out there that the terrorists take advantage of. But at the same time, we have been able to degrade significantly the terrorist threat that we face from certainly al-Qaida core.

But one of the things we need to make sure of is that we’re not going to, after this anniversary passes, when everything is conjured up once again in our minds, that we become complacent. And it’s not a question of, you know, maintaining that sort of exceptionally high level of readiness. It’s a level of vigilance that I think we need to keep as a country, both as a government as well as a people. And one of the things that I think this country has done well over the past decade is ensure that this is going to be a whole-of-government effort and a whole-of-nation effort.

There has been tremendous strides that have been made as far as the integration of information between the intelligence and law enforcement and homeland security communities. There is robust interaction between the federal and state and local elements, the JTTFs and the fusion centers. We’re not still there – it’s not the perfect architecture as far as the flow of information and electrons, but we’ve come a long, long way.

And in many respects, I think this demonstrates the ability of two successive administrations to enable and empower the counterterrorism community to accomplish what it needs to accomplish. The CT professionals that are out there on a daily basis, working, you know, harder than the American people understand, whether they’re at airports, whether they’re at embassies abroad; whether they are, you know, in a JTTF, pulling the latest threat piece that comes in, there has been tremendous work that has been done.

So when I look back at the last 10 years, I feel really good about what this country has been able to accomplish. The fact that we’ve been able to prevent another calamitous attack like was on 9/11 – but at the same time, we recognize that al-Qaida is still out there; there are other groups that are trying to carry out attacks here. Although al-Qaida core in the FATA and Pakistan has been significantly degraded, we do have the metastes (ph) of al-Qaida in Iraq, in Yemen, in the Sahel in Africa, in other areas.

But it’s – we’re not going to relent. One of the things that President Obama has said is that we need to do everything possible to protect the American people. We need to do it consistent with our laws, consistent with the values that we hold dear, but we need to make sure that we’re working very closely with our partners overseas. And that’s the other big difference that I see over the last 10 years: The international partnerships that have really blossomed.
Ten years ago, there were a lot of countries, particularly in the Middle East, that were in denial. And I think, you know, Saudi Arabia was one of those. And Muhammad bin Nayef, who we both know and respect tremendously, acknowledges that Saudi Arabia was in denial at that time. They realized then after, you know, attacks within the kingdom in 2003 that they had a real cancer within their country. And they then took the steps that were necessary to, you know, prevent al-Qaida from using Saudi Arabia as a base for attacks, both there as well as outside.

So the capacity building that we’ve done in other countries, working very closely with our traditional partners and allies but also establishing close relationships with other countries, giving them the intelligence information that they need, giving them the training, letting them know how we have been able to make progress against al-Qaida – I think these are all things that as a country we should feel proud of. And many people who are here today, I think, can take pride in the work that you have done, either in the government or in the private sector to allow this whole-of-government, whole-of-nation effort to flourish.

MS. TOWNSEND: John, I should – I’d like to – before I begin the questions, I should both congratulate you, the president, the administration. Having sat in your seat for some time, I understand at a very personal level the courage and strength it took for the president to make the decision he made to authorize that raid into Pakistan. Unless you’ve sat in these seats, I don’t think people fully appreciate the burden on the president and the responsibility, the weight of that responsibility at that moment. And so I think I speak for a lot of people in this room when I say the nation owes him and you a debt of gratitude for that successful raid. And we are certainly as a country safer for the killing of bin Laden. So thank you. (Applause.)

MR. BRENNAN: Well, as you know, the real credit goes to those very brave operators that carried out the raid, those very dedicated, diligent and extremely proficient and expert intelligence officers that were able to pull the thread over so many years; and then to the president, who, you know, was able to take that information in, both in terms of what we knew about it, which was circumstantial; but also I think it reflected the tremendous confidence that he has in the U.S. military, as well as in the intelligence services.

And yes, you know, the intelligence failures are talked about quite a bit. And, you know, sometimes policy failures are attributed to be intelligence failures and vice versa, but I think that the president felt as though we did as good a job as possible, we the U.S. government, as far as being able to understand what was happening in the compound in Abbottabad, that we were going to – we basically had as much information as we could get securely without risking the potential operation. But at the same time, these operators have trained and have carried out these types of raids repeatedly.

And one of the things that after the bin Laden raid that I’ve heard many, many times from our foreign partners is that they’ll come up and say, you know, only the United States could do that. You know, it really was, you know, a way to demonstrate that the United States has that determination, that persistence and the capability to project that type of capability to another part of the world and do it efficiently and effectively and, you know, secretly. And that’s one of the things we were all impressed with, the fact that the U.S. government can keep a secret, and that
was something that the president insisted on; and, you know, the compartmentation that is necessary for that and doing it in a way that ultimately led to success.

But it’s not one person, it’s not one group of operators or group of intelligence analysts. This is the product, I think, of work that was done tirelessly over the last decade. People have been going after bin Laden for a couple of decades. And it was a time of reflection but also a time of, I think, remembrance of the victims and – this was something that – this was justice, this was something that the American people wanted and deserved.

MS. TOWNSEND: Tell us, John, now post the killing of bin Laden, how does that affect the threat? How do you see the current threat to the United States? Will al-Qaida seek to retaliate? Do they have the capability of retaliating?

MR. BRENNAN: Well, we were – when we went into the compound, we were able to take some of the materials out of there, it was quite clear that bin Laden was heavily engaged in trying to direct operations. If anything, I think it also reflected his – you know, how much he was distant from reality in terms of what al-Qaida, you know, could do, because he kept pushing for these operations, large operations, but the al-Qaida organization, because of the depletion and operatives and because they couldn’t train, they weren’t able to carry out those attacks.

What I think, looking back over the past several months, there’s been a combination of events that really, I think, have set al-Qaida back a lot. It was bin Laden, it was Ilyas Kashmiri who was killed shortly thereafter; it was Atiyah Abd al-Rahman, who was, you know, very, very active and engaged and the person of al-Qaida core who was really orchestrating a lot of activities, whether it be in Yemen or the Sahel or other areas; Younis al Mauritanis that the Pakistanis announced were arrested, who was responsible for external plotting – these are the senior types that had the experience, they had the respect, they had the ability to orchestrate the organization. You take them off, now you have, you know Ayman al-Zawahiri and you have, you know, a few other guys, Yahya al-Libi and others, that still are out there. And we’re going to be relentless as far as going after them.

But al-Qaida core, the senior leadership in the FATA, really has taken some severe body blows. We need to maintain that pressure. And, you know, hopefully we’re over the real speed bumps that occurred with the Pakistanis because of the raid against the bin Laden compound. And I think it was demonstrated by the Younis al Mauritani capture.

But we need to do things not just in the FATA. We’re going to keep pressure there, but, you know, al-Qaida in Iraq is still very active and is attacking our troops. And al-Qaida in the Arabian Peninsula is, as we say, the most operationally active franchise that is out there right now. And they both have a domestic agenda in Yemen, and it’s taking on many, many characteristics of a traditional insurgency as it has pushed Yemeni forces as well as civilian government out of areas of Abyan in the southern portion of the country. But then you have people within the organization like Awlaki who are determined to carry out attacks against the homeland. So, that both has a domestic and an international agenda. Al-Qaida in the Islamic Maghreb, you know, is there and then looking at Libya and the arms bazaar that is available there.
So, you know, the threat is still evident. The Arab Spring has resulted in some upheaval in a number of countries as far as the counterterrorism security forces. The Egyptians that have been a very, very close partner of ours over the years – their services have been, you know, affected significantly by this recent turmoil.

So I think the effort needs to continue. The challenges are still there. But I think we’ve put in place a good foundation in a lot of these countries that have been able to withstand some of these, you know, political upheavals. So we’re building some of them back up. And, you know, we’re – we had a CT relationship with the Libyan government. We have close relations now, obviously. We recognize the TNC and Libya. We need to make sure that we’re able to work with them, again, building their capacity, because we rely on these countries very, very heavily.

And one of the – I’ve been asked recently is, you know, why don’t we capture more of the terrorists that we did, you know, early on and they all went to Guantanamo? Is it because we’re not capturing them anymore, we’re just killing them? No. We capture them when we can. Warsame is a good example that was a Somali, who was in Yemen, we captured and is now in the United States facing trial.

But we now rely and are able to rely heavily on a lot of these other countries, you know: Saudi Arabia, the Emirates; you know, the Moroccans, the Egyptians and others who are now doing what they need to do. And so we don’t need to do these things unilaterally. We work very closely with them so they can, you know, find, detain, arrest, try, imprison the terrorists that are a threat to them as well.

MS. TOWNSEND: And when other countries take these people into custody, do we get access, do we get the intelligence related to the U.S. homeland?

MR. BRENNAN: Many times. And whenever there is a terrorist that is captured, we – the first thing we do is we ask for that kind of direct access, whether it be in Pakistan or whether it be in Yemen or Saudi Arabia or other places. And usually, the countries and the services work with us, you know. There are obviously some concerns that some of these countries have if, you know, there are concerns that they have about what the individual might reveal to us, but I think it’s very important for us to be able to have that direct access so that we are able to determine what this individual is saying, how they’re saying it, not under duress or coercion.

And so I think the relationships have developed to the point where, you know, more times than not we’re given that type of access according to their rule of law as well as ours.

MS. TOWNSEND: Let’s go back for a moment to the – to kind of the post bin Laden threat. You know, over the last week or 10 days, DHS, the Department of Homeland Security, issued its sort of 9/11 warning. There was the State Department worldwide warning to Americans traveling overseas. This morning, the Department of Defense raised its threat level to bravo here in this country.
And so as Americans watching this, we know that there was some reference to a 9/11 anniversary attack at the Abbottabad compound from public reporting. What does this mean? Are we – are you concerned about an anniversary type attack? And do you see increased threat reporting right now around the anniversary?

MR. BRENNAN: Well, if you remember last year, there was a spate of reporting about plans to carry out attacks in Europe. And there were a number of measures that were put in place in Europe because we had very specific and credible information that led us to work with those European governments to institute additional security measures and put in place.

Now we have seen things like in the – you know, the bin Laden compound, where references are made to 9/11 anniversary. We know that there have been times when they tried to take advantage of the attention paid to these anniversaries. But usually the operational activities are timed to take place when they’re ready, as opposed to, you know, forcing it to take place on a day.

But we need to make sure that we’re doing everything possible to prepare and to safeguard this country. So out of a, you know, abundance of caution and prudence, we have instituted a number of things this week and over the weekend, where the FBI, Department of Homeland Security, Department of Defense are – Department of State, you know, issues alerts, advisories. We want to make sure people are aware that this could be an opportunity, that terrorist groups might try to take advantage of the large gatherings of people as a way to demonstrate that they can penetrate our defenses. So one of the things that the president has insisted – and I know President Bush did the same thing – make sure we do everything possible before, you know, an anticipated either, you know, anniversary or time so that we’re best positioned to catch something before it actually comes to fruition. And that’s what the case is here.

But right now – and, you know, if we did have something specific incredible that would require some type of advisory alert to go out, we would put that out. I think we have come a long way in ensuring that that information gets out to the American public. And FBI and DHS are putting out these bulletins. You know, there was a bulletin put out about threats from general aviation, highlighting the fact that al-Qaida keeps coming back and coming back to using aircraft as a platform or as a target. And this is something that, you know, we need to make sure we maintain that vigilance for.

MS. TOWNSEND: John, I – like you, I had the privilege of working with Muhammad bin Nayef in Saudi Arabia and other intelligence chiefs around the world, but I have wondered in the wake of the Arab Spring where many of the governments, the governments that existed at the time I was there, have fallen. And there are concerns that those that – that this is an opportunity that terrorist groups might take advantage of, whether it’s Muslim Brotherhood in Egypt or al-Qaida in the Islamic Maghreb throughout North Africa.

Can you talk a little bit about those counterterrorism relationships? Should we be concerned that they’re not as strong? How do you view the changes that are taking places, vis-à-vis the counterterrorism mission?
MR. BRENNAN: Well, a couple things. One is that it was clear that al-Qaida was not at the vanguard of any of these movements, whether they be in Egypt or other places. And I think in some respects it, you know, exposed the bankruptcy of the ideology. It’s not having the resonance it hoped to have had, you know, 10 years after 9/11.

But the impact on the CT relationships, I think, has been in certain areas, you know, significant from the standpoint that we’ve had to now work with, you know, new people, new organizations. There is a concern in places like Libya, where there is not the same type of governmental control, there’s a lot of MANPADS and other things that are out there and potentially could be accessed, acquired by the terrorist organizations.

But the professional relationships that exist, for example, between, you know, CIA, FBI, others with their counterparts, those are things that endure institutionally. And although there are changes in personnel, one of the things that, you know, I – when I first noted this was back in the early ‘90s when a number of countries, including Jordan and Yemen, sided with Iraq, you know, when Iraq invaded Kuwait. But those intelligence relationships were able to withstand those political challenges. And they’re endured. And the CT relationships over the years have strengthened so much that that becomes almost the “sine qua non” of the relationship between, you know, CIA and some of the local services that you’re really trying to collaborate against the terrorist challenge that we mutually face.

So, yes, there are some challenges here. We need to be able to continue to work with the Egyptian services. You know, Tunisia has been a mixed record. You know, even before the upheaval there, there were things they were doing that we were unhappy with. And we need to keep pressing.

You know, Yemen is a country that I have become all too familiar with over the past two years. I’ve been out there numerous times. I can say today the counterterrorism cooperation with Yemen is better than it’s been during my whole tenure. Now, that’s a result of a number of factors. One is that the terrorist challenge is really significant there, and al-Qaida in the Arabian Peninsula really has put down roots and it now has insurgency like, you know – (inaudible) – to it. But the information is flowing back and forth. We’re sharing information. The Yemenis have done a good job of finding and arresting and, you know, carrying out attacks against al-Qaida types. So even though Yemen is in the midst of this internal domestic turmoil, that counterterrorism relationship still stays strong.

And that’s so critically important for the United States. We want to do these things in a bilateral way, not unilaterally. We want to be able to work with the services, but that requires their cooperation, that requires that they adhere not just to their legal system but to international standards and norms as well.

MS. TOWNSEND: OK. So twice you’ve mentioned caches of unsecured weapons in Libya, so I’ve got to ask you what we’re doing to make sure that those aren’t taken and used against us or against others.
MR. BRENNAN: Well, we’ve made a number of very clear points to the TNC and those that we’re working with in the Libyan environment right now about the things that we are very concerned about. Obviously, securing any type of materials or weapons that could be used by terrorist groups, whether it be weapons of mass destruction or whether it be MANPADS or whether it be arsenals of weapons – obviously, there are a lot of that country right now that are ungoverned – a lot of concerns.

And so the Libyan – the new Libyan government is going to have quite a challenge ahead of it trying to gain control over those different elements of the country that are a combination of tribes and families and – you know, there’s going to be traditional rivalries that are going to be coming to the fore. But this is where I think the United States does respond very well. We have people who are working very closely with the TNC. You know, we want to be able to get back in there to Tripoli as soon as we can. We want to be able to go back to the embassy, you know, secure the compound, work very closely with them; and once again, you know, have the type of relationship with the Libyans that we want to have with, you know, countries across the region.

You know, when you look at – you know, al-Qaida – and it’s not just the Libyan Islamic Fighting Group that was, you know, a real concern and still has people in different places. But a lot of the senior al-Qaida members are Libyans, you know: Atiya Abd al-Rahman al-Libi; you know, Abu Yahya al-Libi. You know, they’re all – you know, many of them, senior ones, are Libyans.

So it’s important for us to be able to work with the new Libyan government.

MS. TOWNSEND: OK, so I’m going to ask a question. When I sat in John’s seat, it always sort of irritated me. So I apologize in advance. (Laughs.)

MR. BRENNAN: (Inaudible) – lesson then? (Chuckles.)

MS. TOWNSEND: You mentioned having met with the 9/11 commissioners about their report card. OK, so the irritating thing is you always – journalists will always ask you about the bad ones, not mention the other, you know, what is it, 30 of them that you’ve completed. So I’m going to ask you about – talk to us about the nine that they didn’t give a good grade on, if you will, and what are the priorities there and likelihood that we can sort of close this one out?

By the way, I was unsuccessful at closing it out either, so I ask it with all humility.

MR. BRENNAN: Well, there are some that are within our control and some that are – have different types of challenges. For example, the overhaul of the congressional oversight committee structure; that’s something that there has been not a single sort of move to address in the last decade. That is something that I think needs to be addressed. It’s tough, though. You know, I’ll give it to the Congress that, you know, there are a lot of rice bowls there. But aside from that, you know, the intersection between homeland security and intelligence and law enforcement and defense is quite challenging. So doing that, I think, is important to do; they need to do it thoughtfully. And I think they had waited because at the time that the 9/11 commission recommendations came out, they wanted to executive branch to overhaul itself with
the Office of the Director of National Intelligence and the NCTC. But then it was a can that kept getting kicked down the road.

The other – you know, one of the other areas is the Privacy and Civil Liberties Oversight Board, the PCLOB, which is something that is a, you know, presidentially appointed group of folks that would oversee for the U.S. government the privacy and civil liberties issues. We have not been able to stand that up since this administration’s come in. We had a number of people that we were trying to get to be the chair of that, and there – various, you know, things happened that – you know, we don’t have somebody yet. We’re working on that. We have, you know, identified a couple of members that we want to have on there. But even though we don’t have the PCLOB, there are privacy and civil liberties officers at each of the departments and agencies. And they are very active. They work collectively as a group. I mentioned to the 9/11 commissioners that I’m going to be getting together with them next week to talk about making sure that they’re empowered, that they feel that even though there’s not a PCLOB structure, White House, that they are able to do their jobs.

You know, there are issues of REAL ID in terms of what the federal government is requiring of states. But states can pass their own laws that make certain things not permissible. So there’s this, you know, Hamilton/Jefferson challenge still that we’re facing.

And biometrics – that’s something that – you know, it’s an evolving arena that we need to, you know, stay very much focused on, making sure that we’re able – one of the things that they pointed out that we don’t have the processes in place to collect the information on exit from the United States.

So these are things that we need to continue to work on. But when I look at some of the real fundamental recommendations of the 9/11 commission, I think between, you know, the two administrations over the last 10 years, you can check off a lot of them and say, boy, we really have come a long way. So, you know, the fact that we still have some things to accomplish out there, we need to stay focused on them, but I like to look at those things that we were able to put in the win column.

MS. TOWNSEND: Let me ask you – folks here this morning will know exactly what my next question is. This is my hobby horse of the ones that are not accomplished yet, because I really worry about the consequences of it. And that is the additional bandwidth for first responders. There is a bill pending before Congress that the president has supported.

Question to you is, one, what is the likelihood it will pass, given all the other things facing Congress right now, not least of which is the budget concerns and fiscal concerns; and second, is the president willing to make it a presidential priority to get this thing passed?

This is – again, this – there’s two administrations here, and it hasn’t gotten done yet. But people will be hurt and people will die if we don’t get this thing – get this thing done.

MR. BRENNAN: Yeah, and it’s one of the things the 9/11 commissioners did point to. And yes, there is the D-block, and making available to those first responders in the state and
local communities. But there’s also the build-out of it that’s required in order to make sure that it is going to be, you know, servicing that.

But there also are issues related to – you know, you have an interoperable system; you want to make sure that you have the systems engineering in place as far as the business model or the orchestration of that. It’s not – just being able to communicate with everybody in itself can lead to a very chaotic and – environment if there’s no system in place that will allow the – that there’s going to be some orchestration of that interoperability and connectivity.

So the – in event of another 9/11, one of the real problems was there were so many people on the net, weren’t able to distinguish – and, you know, it was almost overloaded. So you need to make sure that you’re able to build out a system that will be able to leverage that interoperability and that bandwidth in the spectrum.

The president is committed to making sure that he’s able to do what can be – but as you know, it’s – there is a big congressional stake in this; there are a lot of different sort of equities as well as perspectives on this. You know, should we be making more progress on this front? Yes. Should we be able to have an interoperable system that is going to be within some type of business architecture that will allow communication to take place, certainly in emergency situations but not so that the airwaves are inundated with everybody who can access those channels? That would just lead to, you know, anarchy.

MS. TOWNSEND: John, talk to us for a moment about your view of how intelligence reform has been implemented and how it’s working. You’re on – I think the administration’s on your second DNI – Jim Clapper will be with us later today. What is your view of how intelligence reform is working?

MR. BRENNAN: (Pause.) I pause because there, as – you know, how is it working now, and what does it need to do as far as the future is concerned? Jim Clapper has, I think, been outstanding. And he has tremendous breadth of experience in the intelligence community over the years, and he, I think, has the right touch. He’s not trying to be overbearing, but at the same time he recognizes that there needs to be an integrated community here.

So I think the changes that have taken place have been in a positive direction. The real challenge, and the rub – and this is one of the things the 9/11 commissioners noted as well – is that the DNI needs to have more control over personnel and budgets. Well, those personnel and those budgets happen to be in departments and agencies that have their own cabinet officials or agency heads with their own appropriators. And so it’s easy enough to say, well, the DNI should be in charge of all the intelligence community that’s scattered throughout these 16 or 17 departments and agencies. But the practical implementation of that, I think, is challenging.

You really want to take away from, you know, the secretary of state or the secretary of defense a large chunk of their workforce, and so the DNI will then make determinations based on what national requirements are. They have their departmental requirements as well that the intelligence mission is supposed to be able to service.
So the – one of the things that Jim is trying to tackle also is the whole IT area, and that’s – on intelligence reform, making sure that you have an interoperable system there so that you don’t have, you know, wasted resources and systems that are not able to be integrated. But you’re going to have the appropriate systems in place that you take into account cybersecurity, compartmentation, other types of things – a lot – a lot – of money, as people know, go into the whole IT structure.

MS. TOWNSEND: Bringing you water. (Chuckles.)

MR. BRENNAN: I was afraid – it wasn’t a note. (Chuckles.) I don’t want to have a note. (Chuckles.) Notes are never good in my business. (Chuckles, laughter.) It’s what the president says to me, too – he says – (each time ?) I open his door, he goes, oh, no, Brennan’s here again. Oh. (Chuckles.) It’s not good news.

MS. TOWNSEND: President Bush had the same reaction to me.

MR. BRENNAN: (Chuckles.)

MS. TOWNSEND: Talk to us for a moment – you know, one of the things in the stand-up of the Department of Homeland Security was the intelligence and analysis capability. What’s – you talked about the DNI’s role; what is the DNI’s appropriate role when it comes to homeland intelligence? And how has that intelligence capability at the department built – and how effective is it?

MR. BRENNAN: Well, you know, the Department of Homeland Security has, I think, a very unique responsibility because that’s really where, you know, the threat and vulnerability information really needs to come together so that we’re able to map it in a way that the Department of Homeland Security can take the appropriate actions to mitigate those threats and to mitigate those vulnerabilities.

And so there are different components, obviously, within the Department of Homeland Security – intelligence and analysis directorate there; and Karen is doing a great job. She needs to make sure that the secretary has full visibility into those threats and vulnerabilities that, you know, the secretary is responsible for addressing.

And so, for example, yesterday we got together; the president has these biweekly sessions with the heads of the different departments and agencies responsible for counterterrorism – so, you know, Defense and State and Homeland Security and FBI and CIA and others are there. We went over the 9/11 anniversary preparations, and we addressed the threat; we talked about what we’re doing with our partners overseas; we talked about what the FBI is doing here with JTTFs.

And we finished up, and rightly so, with Secretary Napolitano, who is going to say, OK, now, in light of all of that – in light of the threat, in light of the engagements that we’ve had, this is what we’re doing to ensure that we are as best prepared as possible to protect the homeland. That has to be informed not just by the intelligence community writ large, but this is where I&A really needs to be able to help Janet and others be able to identify those things here in the States.
that if the threat – latest threat vector is coming from, you know, the FATA, and it’s focused on bridges or tunnels, these are the things that we should be thinking about in terms of steps that we can take – what we need to do as the department so that we can address the vulnerabilities, working with state and locals.

So you know, what I&A is doing inside DHS, it shouldn’t be a replication of what NCTC is doing, which is just packaging of the threat; it’s really taking that threat, announcing, OK, the DHS mission is this. We need to make sure that we’re able to, again, map it against that mission so that the secretary knows, OK, there are certain policy initiatives we need to take, certain measures we need to take, or additional security precautions.

MS. TOWNSEND: And what is the DNI’s appropriate role when it comes to homeland security intelligence?

MR. BRENNAN: I know that INSA issued a white paper this morning, and – (chuckles) – and don’t ask me about it because I haven’t read it yet. I did read sort of the top lines there. And you know, there’s homeland security intelligence, which is what the white paper focuses on. And I don’t know whether or not it’s being used synonymously with homeland security information. To me, that’s the broader universe of information that is out there – intelligence conjures up something that’s acquired clandestinely or whatever – but that homeland security information consists of many different components; there are things that will be acquired by, you know, law enforcement and investigators, or at the border, you know, as people write out their applications, or from intelligence that’s collected.

And so I think the DNI needs to make sure that the – that the intelligence community as a whole is able to provide to Bob Muller, to Janet Napolitano, to others who have responsibilities for protecting this homeland that the intelligence machine is able to collect and analyze information in the best way possible that will allow them to do their jobs.

The president looks to them to make sure that they’re able to uncover the threats or to, you know, address the vulnerabilities that exist here. They need that intelligence support; they need to be able to ensure that they have full visibility so they can take the appropriate steps. So Jim Clapper, in my mind, needs to be sure that our collection systems, our analytic systems are really hitting on all cylinders in order to give those two organizations – FBI and DHS in particular, but others as well – what they need.

Now, that doesn’t mean it’s, you know, clandestinely acquired, whether it be technical or human. And open source is a great example of what we need to be able to do to leverage. And social media that’s out there – you know, there’s a whole new universe of information that’s available now, some things that are available to private sector that aren’t available to, you know, the intelligence community because of certain laws.

But I think what Jim Clapper and the intelligence community have to do is making sure that that universe of information that’s relevant to homeland security is made available to Bob Muller, Jan Napolitano, and others.
MS. TOWNSEND: OK. So you mentioned both the FBI and DHS. When we talk about sort of homeland-related threats and information or intelligence, there has been much written and much talked about the tensions that are inherent in that relationship. Is it working better? And who – in your example, if there’s a threat against bridges and tunnels, who is both responsible and accountable for passing that to – I now live in New York – to Ray Kelly, who’s the commissioner there, or to state and local authorities?

MR. BRENNAN: Well, if there is threat information – a lot depends on where it’s acquired. But for example, let’s say if there is a human source that’s reporting out of the FATA – and so, let’s say CIA somehow gets – acquires that information, it comes into the system, and it will immediately be disseminated. It’s one of the things that I think CIA has done a great job of, making sure that that type of threat information is immediately available to others.

It goes out and will be made available, then, on FBI systems as well as DHS systems. It will be immediately available at the JTTF in New York. That’s from the standpoint of, if there’s a threat to a bridge or a tunnel or something, and there’s an operative (here ?) in New York, they need to then use that information to track down that lead.

The JTTF’s mission is not to ensure that there’s the propagation of the information to state and locals, although frequently it’s used for that. But it’s an operational environment that you combine the federal agencies and state and local officials there so that they can run it down.

DHS, in my mind, has the responsibility to ensure that state and local officials, as well as private sector – because the private sector is affected a lot – they have primary responsibility for ensuring that they’re aware of this, and that they can then take the steps. Because it is going to be the state and locals who have the responsibility to step up, maybe, the security – the visible security presence at a bridge or a tunnel, or that they need to do additional checks.

But this is where, you know, I think Bob Muller and Jan Napolitano have a very good relationship. Trying to control, though, dissemination of this type of information, and making sure that people don’t do anything until Janet picks up the phone and speaks to either Ray Kelly, or Bob picks up the phone and speaks to Ray Kelly – it ain’t going to happen. The thing is to make sure that it gets out there and that people are able to take action appropriately. That’s why, I think, the nature of the information that is passed out there really needs to be at the, you know, releasable level.

If the information that was first acquired – it includes some very sensitive operational information that if exposed could compromise source and methods, that is not information that needs to get to state and local officials, in my mind. The fact that there’s a threat, the fact that it might involve, you know, a certain type of person – a descriptor or whatever – that can get out, and that needs to get out quickly. And one of the things that I think Bob and Janet have been very good about is not saying, no, no, no, that’s my job – no, no, that’s my job. They want to make sure they’re fulfilling their responsibilities, but they’re not going to say to someone, don’t share that threat information. That’s the last thing anybody wants to do in the government these days – you know, don’t share that threat information; that’s my responsibility. You know?
MS. TOWNSEND: I think – I think it is fair to say that there has been a lot of progress on information-sharing. But of course, there are – you know, nothing’s perfect, right? And there are inevitable opportunities for failure, as I used to call them. The Abdulmutallab – attempted Christmas Day bombing – information was imperfect, and it was imperfectly shared. Can you talk to us about the progress that you’ve made? The president put you sort of at the point of ensuring the information-sharing improved. Can you talk to us about kind of how it’s improved, and your level of confidence in that improvement?

MR. BRENNAN: Well, one of the things that we have done – I know that, you know, previous administrations have done as well – is that you want to make sure that you’re able to leverage experiences so you can correct any flaws and deficiencies. And the president has insisted, whether it was on the Abdulmutallab incident or the Faisal Shahzad at Times Square or the Fort Hood shooting, that we look back and see what we had available to us, and do the forensics on it, and to say, OK, in light of what we knew before that attack, what could we have done better, or what could we have been able to do if we just had a better system of either information-sharing, or different policies, or whatever?

So in each of those instances, we found examples when either something – for example, in Abdulmutallab, you know, there was a report that was not disseminated, you know, in a timely fashion because the resources on a particular desk were single-threaded. So somebody was away, and so it was there for a day or two. Well, that’s easily fixed: You can flag something; you can make sure that there is going to be backup. You know, the issue about a misspelling that was put in to do a check – those are things that, you know, you don’t realize until it becomes a problem.

The issue of sharing information between the FBI and Department of Defense – it was a big issue as far as the Fort Hood shooting is concerned. This gets to the issue about, you know, personnel files and other types of issues that address, you know, personal liberties, civil liberties. But the DOD and FBI (have ?) put in place a process whereby those civil liberties would be protected, and privacy rights, but at the same time, there would be visibility in a – in a manner across the FBI-DOD wall so that if there’s information of concern that the FBI needs to investigate, you know, we will do it.

We had the recent example of the individual who was going to carry out attacks, again, at Fort Hood, Naser Abdo, who we look back on that and – to see what could have been done differently that would have allowed us, maybe, to identify this individual earlier. Thankfully, there was a very vigilant, you know, store clerk who brought, you know, their concerns to the attention of local authorities.

But I do think that in each one of these instances, it brings to the surface some things that you don’t know are a problem until you experience them. And you know, it sometimes requires IT changes; sometimes it involves systems processes changes. But I think in each instance, all the departments and agencies have been very, very good as far as, you know, explaining what happened because they want to be better.
And I have not found any instance where a department or agency has tried to sort of, you know, cover up anything. That’s one of the things that the president said to folks, I remember, after the Fort Hood shooting. And in the Oval Office, he had the heads of the departments and agencies that were involved and said, listen, I want to get to the bottom of this; I want to find out what happened here. But I want to make sure that we understand, you know, what happened, and I don’t want anybody sort of holding back on this.

And so, you know, sometimes the Congress will do their own investigation; sometimes they hit us for the failures. But what we’re most interested in is making a difference in terms of our future capabilities. Yes, there is an accountability issue; yes, we want to make sure – if somebody, you know, made a mistake despite their best efforts, that’s one thing. If someone was, you know, derelict in their duty, that’s something else.

MS. TOWNSEND: You mentioned IT. Just before we came on, Senator John Warner was on stage and mentioned the threat that really concerns him right now is the cyber threat. Talk to us about your view of the cyber threat, and what we are doing as a country to combat it.

MR. BRENnan: Yeah, as challenging as the – as the terrorist threat is, the cyber threat makes my head hurt even more – it really does – just because of the challenges that we face and the openness of the cyberenvironment. I mean, here we’re talking about an environment or domain that is, you know, privately run, privately organized. And the U.S. government has responsibilities because U.S. government will feed off of that Internet. We want to make sure it’s secure; we want to make sure that we’re able to stop any type of attacks against us, but also, we have an obligation to the American people and our critical infrastructure.

So there are a number of things that are underway – and many of them that started in the previous administration, (and we’re ?) continuing to do – working with the private sector, being able to have the ability to, you know, acquire the signatures of different types of attacks; making sure we’re able to share that information within the government; making sure we’re able to share it with the private sector.

One of the challenges is, particularly in the private sector, is that, you know, we want to make sure that they share their experiences with us when they get hacked. We want them to share it with us. But at the same time, they have their own sort of concerns that if that information gets out that they were successfully hacked, it could have a, you know, an impact on their stock prices.

So what we’re trying to do is to ensure that there is going to be this relationship with the private sector, that they feel confident they can share this information with us, and that we’ll be able to work with them.

And there is a debate right now, and we had sent up to the Hill a legislative package that makes certain – you know, has certain statutory requirements then of, you know, the private sector as well as abilities of the government to do things. We don’t want to put in place a strict regulatory framework that is going to be, you know, a deterrent to innovation and is going to paralyze the system. At the same time, though, the ability of either foreign actors or, you know,
groups or even individual sophisticated hackers to cause damage is serious. And you know, the

cyberfront is a – is a concern.

And it’s an open environment. We’ve made some strides; it’s one of the areas that the

president has really focused on and insisted that we need to, you know, work harder, work faster, work better because of the concerns of the impact on not just our civil liberties in terms of hacking and intellectual property but also on our economic well-being.

MS. TOWNSEND: Does the U.S. government have both the capability and the legal authorities that it needs to combat this threat? And if not, what are the sorts of legal authorities that you think you need?

MR. BRENNAN: Well, the legal authorities were – some of them are addressed in the legislative package. And you know, there are some people who feel as though we need to go even further as far as giving the U.S. government additional capabilities in this area and requirements as far as the private sector is concerned – and more regulation of that. There are ways that I think we can address it.

Do we have the capabilities? The – you know, the technical world, it changes every day. And the capabilities of these hackers and those who are trying to do us harm continue to evolve. We do have, I think, rather significant capabilities. We are doing a number of things. We have a pilot that has been running with the defense industrial base to try to make sure that we’re able to work with them so that – you know, they are subject to being targeted by cyberhackers abroad, whether it’s, you know, other countries or companies that are trying to steal from them.

So I think with these pilots, we will experience certain things. We have to make sure that we’re doing it consistent with, you know, issues related to legal liabilities and whatever. But you know, I think that we need to look very seriously at this environment if we’re going to have it as the backbone of our, you know, daily lives – what really needs to be done there that will make it more secure.

Some folks feel as though the market is going to develop that once it becomes cost-prohibitive for these cyberattacks, because the losses are, you know, billions of dollars. But allowing the market just to evolve in a way that will ensure some additional cybersecurity, I think, is a bit short-sighted. I think there are things that the government can do in collaboration with the private sector that make a lot of sense.

MS. TOWNSEND: Are there specific things that you’d like to see the – being now a member of that private sector, are there specific things that the private sector could do to be helpful to the government? Are there asks that the government has of the private sector in this area?

MR. BRENNAN: Well, part of is just making sure they have the dialogue. And I think the dialogue has been – has been very good with certain segments of the private sector – certainly, aviation industry; a lot of the financial-sector components are very good as well.
I do think it is making sure that these private-sector companies do share with us – and Department of Homeland Security has primary responsibility here – share with us their experiences. We need to understand the different types of attack vectors, the different types of signatures. We need to make sure that we have that visibility into what their experiences are.

But also to, you know, voluntarily do – they can do some things themselves to tighten up their security practices. And there are guidelines and things that we can help them with. But their security is dependent in large measure on the discipline and the rigor that they have in ensuring the protection of their databases, of their critical information that they have. And particularly at a time of cost-cutting with, you know, the economy where it is, some companies will pare back those long-term investments because they want to make sure that, you know, they’re able to do what they need to do this week.

And if they’re paring back those cybersecurity investments, I think they’re doing it at their own peril. They need to continue to focus on that and devote their – appropriate resources to it.

MS. TOWNSEND: John, last question – I mean, no conversation at this time would be complete without sort of acknowledging and asking you about the impact of the current fiscal crisis. There is great concern – you know, in the wake of the Cold War, starting with Bush 41 and through Clinton, there were tremendous budget cuts in the national security apparatus – the military, the intelligence community, the law enforcement community. That’s been built up pretty steadily over the last 10 years to give us the current capability.

There is tremendous concern here and, I think, nationally about what are the implications for our national security capability in this time of tightening budgets. Can you give us a sense of what to expect in terms of budget cuts?

MR. BRENNAN: Look, clearly, all of the U.S. government departments and agencies are going to have to be part of the effort to trim budgets so that we can, you know, live within our means. The tremendous investment in intelligence as well as in Iraq and Afghanistan over the years has been very, very significant. And as we wind down in Iraq, and as we (ph) now looking at Afghanistan, we have to make sure that we’re able to have the capabilities that will ensure that the investment that was made is going to allow us to do what we can to work with our partners – the Iraqi government, the Afghan government, whatever.

I do think this is where Jim Clapper’s role is going to be particularly important. He needs to look out into the intelligence community and make sure that there’s no unnecessary redundancy. And you know, you need to have redundancy, but it needs to be thoughtful, it needs to be deliberate as opposed to unnecessary.

I think you also have to look at some of these very sort of big-ticket, you know, items – you know, some of the technical programs, whether we’re talking about satellite architecture – you know, what we need to do is to make sure that we’re focused on not the capability, but what is it we’re trying to accomplish, you know, and make sure that we’re able to achieve those missions almost irrespective of the platform or the capability.
And sometimes – and you know, we know that Congress will have certain pet projects, as well as agencies will have pet projects. We need to make sure that they are useful, meaningful, important and necessary for the mission that lies ahead of us. And you know, it’s – sometimes, it’s a lot easier in Washington to start a project rather than sunset it.

But some things, you know, serve their time. And that’s why I give Bob Gates a lot of credit for – in the Department of Defense, he made some really tough decisions that – you know, it resulted in a – (inaudible) – cry against him. But these were big-dollar savings, and he was able to reinvest it in other parts of the Pentagon. And I think this is where Jim Clapper needs to make sure that he looks out over the, you know, U.S. government and says, OK, what are the real intelligence priorities there? We talked before about homeland security information – that is critically important – wants to make sure that there is going to be the capabilities that exist, and are – and are resourced appropriately for that.

And again, then, on the IT front, there is a lot, a lot of money invested in IT. And I think as we move forward in some of these new areas, whether it be cloud computing or, you know, integrated networks and systems, there are savings that, I think, can be achieved.

But we don’t want to hurt ourselves in terms of what the American people expect and want from the intelligence community. But I do think that – you know, having somebody who can sit on top of it and say, you know, this was – you know, it served its time, served a useful purpose during its time, but now is the time to sunset it.

MS. TOWNSEND: John, let me thank you for your time today. Let me thank you for your service. And I think everybody here wishes you every continued success.

MR. BRENNAN: Thank you. Thanks.

MS. TOWNSEND: Thank you. (Applause.)

MS.: I want to thank John and Fran for that very insightful section, but I really want to thank John for hiring me, and for Fran for not firing me. (Laughter.) That’s what it’s all about.

This is now time to break for lunch. A couple of announcements: For the members of the press, I understand that some of you wanted to touch base with Fran. She’ll be available at 1:30 for a couple of minutes in the press room. So if you want to talk to Fran, that’s the time to do it.

Lunch is in the ballroom; it’s at 12:15. To get to the ballroom, for those of you who are having trouble navigating this building – because I know I am – when you exit, you’re going to head to the right and there are going to be a number of guides who will be there to walk you to the ballroom. If all else fails, follow the signs that say “atrium,” and you will be there.
Seating is open for everybody but our sponsors. Sponsors have reserved tables, so if you’re a sponsor, please look for your seat.

General Hayden and John Hamre will start at 12:30, so please try and get your lunch by then. And I look forward to seeing you back here at 1:30 promptly. Thank you all very much.

(END)