

Key Excerpts

“Common Threat, Collective Response: Protecting Against Terrorist Attacks in a Networked World”

**Sec. Janet Napolitano
Wednesday, July 29, 2009
Council on Foreign Relations**

- President Obama has been a forceful advocate for seeing the threat of terrorism in all its complexity, and in bringing *all* our resources, not just the federal government, to bear against violent extremism.
- We must therefore refocus our counter-terror approach to make it a shared endeavor . . . to make it more layered, networked and resilient . . . to make it smarter, and more adaptive.
- We must get to a point where we are in a constant state of prepared, not a constant state of fear.
- A wise approach to keeping America secure should be rooted in the values that define our nation, values like *resilience, shared responsibility and standing up for what's right*.
- Today, we face a networked enemy, and we must meet it with a networked response. Therefore, more than just more hardware, we also need new thinking.
- So, how do we secure our homeland while maintaining true to our values? *With four levels of collective response*.
 - It starts with the American people. From there it extends to local law enforcement, and from there, up to the federal government, and then, finally, out beyond our shores, where America's international allies can serve as partners in our collective fight against terrorism.
- Yet we can't hermetically seal off the country, or our citizens around the world.
- The team we put on the field needs to be bigger, better networked and better trained.
- To sum up, countering the terrorist threat is not just the efforts of one agency, or one element of society. Nor is it the consequence of one tactic. Rather it requires a holistic and unrelenting approach: all levels, all tactics, all elements of society.



Remarks by Secretary Napolitano at the Council on Foreign Relations



Release Date: July 29, 2009

New York, N.Y.
Council on Foreign Relations

Secretary Napolitano: Well, good morning and thank you very much. I want to thank Paul Steiger for your kind introduction.

And I want to thank the Council on Foreign Relations (CFR) for hosting us today. I see Steve Flynn here. Dr. Flynn, like several of his colleagues at the council, have been doing some very thoughtful work on homeland security. And I'm deeply appreciative of that. As a council member myself, it's good to be back here. The last time I was here was with Governor Haley Barbour on a panel on immigration.

Now, I must admit that in the Department of Homeland Security (DHS), it is somewhat of a large government department. So we are undergoing what we call efficiency review, looking for ways to make sure that we spend every dollar, every penny we get, wisely. So I thought I would bring my CFR membership dues here today, so I could save the cost of postage. So Paul, I'll just leave these here for you.

Now, the council is an institution I deeply appreciate, because it's one of the rare places where people will show up early in the morning, at breakfast time, to hear about threats of terror and government response. And this will be the highlight of your day.

But alas the topics that we are discussing are with us and are the challenge of a networked 21st century. And so it is important that the council be apprised of what the Department of Homeland Security is doing to meet those challenges.

Now, President Obama has been very forceful about seeing the threat of terrorism in all of its complexity and in bringing all of our resources, not just the federal government, to bear against violent extremism.

So today, I will speak candidly about the urgent need to refocus our counter-terror approach to make it a shared endeavor—to make it more layered, networked and resilient—to make it smarter and more adaptive and to make sure that as a country—as a nation—we are at the point where we are in a constant state of preparedness and not a state of fear.

The challenge is not just using federal power to protect the country, but also enlisting a much broader societal response to the threats that terrorism poses.

Now, a wise approach to keeping America secure should be rooted in the values that define our nation—values like resilience, shared responsibility, standing up for what is right. These are the values that led us to fight and win two world wars—that were on display in the dark days after the September 11th attacks. We must embrace them again now.

So how do we secure our homeland and stay true to our values? We do it with four levels of collective response. It starts with the American people. From there, it extends to local law enforcement, and from there up to the federal government, and then finally out beyond our shores, where America's international allies can serve and do serve as partners in a collective fight against terrorism.

In the last four weeks alone, I have traveled nearly 30,000 miles, from Islamabad to Seattle, engaging partners in all of these levels. We have brokered international agreements, launched new partnerships and challenged our citizens to play their part in our collective security. We face a common threat; it requires a collective response. And we must face that threat and coordinate that response in an evolving and highly networked world.

So the networked world takes on many forms. The cyber-network that runs our power grids, fires our critical infrastructure and facilitates commerce is now a target and is itself vulnerable to attack. This networked climate forces us to rethink how best to protect our values and our security in a world where the tools for creating violence and chaos are as easy to find as the tools for buying music online or restocking an inventory.

We also live in a mobile world, with complex networks of people and information. We cannot forget that the 9/11 attackers conceived of their plans in the Philippines, planned in Malaysia and Germany, recruited from Yemen and Saudi Arabia, trained in

Pakistan and Afghanistan, and carried them out in the United States. So that's why our homeland security network must be built to leverage force multipliers: the cooperation of our international allies, the full powers of the United States federal government, the vigilance of the police on the beat and the untapped resources of millions of our own citizens.

Later today, I'll assess progress at Ground Zero, a special place for our country and a poignant one for the Department of Homeland Security, which was created as a response to the 9/11 attacks. Last Friday I met with Governor Tom Kean, Congressman Lee Hamilton, former Homeland Security Secretary Tom Ridge and others to discuss progress made in the five years since release of the 9/11 commission report.

There, we're right to note our achievements. Progress toward a more secure homeland doesn't belong to one political party; but indeed, much has also changed in just the past six months since I became just the third secretary of Homeland Security, after my distinguished predecessors Tom Ridge and Michael Chertoff.

So let me give you a sense today of how I see the threat environment that we are in—talk about what we're doing to counter that threat in the four response areas I just identified.

So, what does the world we face look like today? First, while the terror threat is ever changing, it is critical to reiterate that the threat remains. The consensus view of the intelligence community, of which DHS is a member, is that the terror threat to the homeland is, quote, "persistent and evolving."

In my daily briefings and as a member of the president's National and Homeland Security Councils, this is something I discuss with the president and the rest of the security team on a regular basis. And so we're constantly looking for ways to better share information up and down the response ladder I just described, from individuals and communities to local law enforcement, to the federal level and then at the international level.

The broader context here is that we've invested considerably in our border and port security and have substantially reorganized the federal government to focus better on the threat of terrorism.

Now, at the same time, there have been continued attacks against our allies and our interests. And make no mistake, Americans continue to be targeted in terror attacks. Just two weeks ago, American hotels were the target of bombings in Jakarta that killed eight people and injured six Americans. Six Americans were among the 164 people killed in the attacks in Mumbai in November of 2008. Three Americans were among the 54 killed in the attack on the Marriott Hotel in Islamabad in September of 2008.

So if 9/11 happened in a Web 1.0 world, terrorists are certainly in a Web 2.0 world now. And many of the technological tools that expedite communication today were in their infancy or didn't even exist in 2001.

So therefore, more than just hardware, we need new thinking. When we add a prominent former computer hacker to our Homeland Security Advisory Council, as I just did, it helps us understand our own weaknesses that could be exploited by our adversaries.

And the threats we face are by their very nature asymmetrical. Terrorism more often has become privatized violence—does not rely on links, links to an army or to a sovereign state.

We often hear that this is what our globalized era looks like, but what is most salient about today's environment is that it is also networked. And in a networked world, information true and false moves everywhere all the time.

And in that networked world, everyone who is part of the network, meaning all of us, can enjoy the tremendous benefits, but also must be ready and willing to learn about and help address the vulnerabilities that come with these benefits. So the team we put on the field needs to be bigger, better networked and better trained.

What are the implications for this network world for the Department of Homeland Security? It means that we must continue to take an all-hazards approach to preparedness, meaning we prepare for natural disasters as well as terrorist attacks. We need to comprehend and anticipate an expanding range of threats.

The threat of a nuclear or radiological device is of grave concern, and reducing that threat is a key administration priority. But we must be equally prepared for biological or chemical threats, which are capacities al Qaeda has sought for years.

We've seen greater use of IED's and suicide bombers in terrorist attacks around the world. And given our responsibilities for enforcing our immigration laws and protecting our ports of entry, we are also keenly aware that illegal immigration is not only a matter of sovereignty but could pose a national security threat as well. The reality that potential terrorists could use a variety of ways to enter the country illegally—fake documents, visa overstays and even border tunnels—make this so.

Now DHS monitors and shares information about potential homegrown threats as well. These can be individuals, radicals—radicalized by events abroad, or lone-wolf attacks.

And last, but certainly not least, we're spending considerable time and attention on the cyber world. Under the Obama

administration's new cyber plan, DHS retains the lead role protecting the government's civilian sites while working closely with the private sector as well.

So what this range of threats shows is that while the shock and pain and images of 9/11 stay with us, the terror threat is even more decentralized, networked and adapted than on 9/11. The terrorists in Mumbai, for example, made use of GPS devices, satellite phones, mapping websites, like Google Earth, and even live cable TV.

Now we cannot hermetically seal off this country, the United States, from the rest of the world. So for DHS to be the best in the world at what we do, we have to multiply the effect of our forces and at the same time promote a global environment that is inhospitable to violent extremism.

Beginning at his Inauguration and continuing most recently at his historic speech in Cairo, President Obama has begun a different kind of dialogue with the Muslim and Arab worlds, recognized there is far, far more that unites than divides us. At our department, our Office of Civil Rights and Civil Liberties (CRCL) is building stronger relationships with Arab and Muslim Americans, as well as South Asian communities across the country, so we can share information with community leaders in a timely manner and also become more culturally attuned to issues that members from these communities often face.

So what is the right response, and what are we doing? As I mentioned earlier, there are four layers, and the place we start is the work of engaging the American people in our collective effort. I'm often asked if complacency is a threat in the United States, and I believe the short answer is yes. But I think a better question is this: Has the United States government done everything it can to educate and engage the American people? The answer there is no. For too long we've treated the public as a liability to be protected rather than an asset in our nation's collective security. And this approach, unfortunately, has allowed confusion, anxiety and fear to linger.

Let me stress—this is no small matter.

This is a first-order issue for us. The consequences of living in a state of fear rather than a state of preparedness are enormous. We may be better prepared as a nation than we were on 9/11, but we are nowhere near as prepared as we need to be. There are, of course, aspects of countering the terror threat that are inherently governmental, but the smart government is one that knows what it does best and which helps others do their best as well.

So here's how we're looking at this. First, with respect to individuals and the private sector, we're taking a much closer look at how we can support and inform our greatest asset, individual citizens, and with them the private sector. You are the ones who know if something is not right in your communities, such as a suspicious package or unusual activity.

Three years ago, it was an attentive store clerk who told authorities about men trying to duplicate extremist DVDs. This led federal agents to eventually round up a plot to kill American soldiers at the Fort Dix army base here in New Jersey—in New Jersey.

Just last month, a—just last month, a passenger saw two employees exchange a bag at the Philadelphia airport that had not been properly screened. That passenger's vigilance ultimately stopped a gun from getting onto the plane.

So there's no doubt that building a culture of preparedness in our communities will require a long-term commitment from all aspects of our society. But there are, as I said, simple ways for you as individuals and community and business leaders to engage right now. With basic training, every one of us can become better first preventers as well as first responders.

You can use ready.gov to make an emergency plan for your family. You can volunteer by contacting your local CitizenCorps or AmeriCorps councils. You can get free training on basic disaster response by joining a local CERT, or Community Emergency Response Team.

Second, we need to find new ways to work with the private sector to become more resilient to disasters of all kinds. And a key piece of this is securing our nation's critical infrastructure. This might sound just like a challenge for the government, but the fact of the matter is, 85 percent of our critical infrastructure is owned by the private sector. And these are critical. These are commercial facilities, chemical plants, emergency services -- much of it owned, as I said, in private hands. We must therefore be more effective at defining our critical assets and providing our private sector and their leaders with the knowledge and technical assistance to help them secure these assets.

Since the year 2003, DHS has issued more than \$28 billion in grants to help secure critical infrastructure at the state and local level, but it has to be more than dollars. It has to be the active engagement of employers who work with us, who work with the federal government and DHS to identify resources and plan for ways to secure them.

I recently appointed a task force to review our existing color-coded threat system. That was the system originally designed to inform the public, and different economic sectors within the public, about impending threats. That review is under way, and I mention it only to say that if a better, more effective system can be found, that will be used instead of the current color-coded one, just to see how—the federal government and DHS rethinking what it needs to provide active information to individuals, to businesses, to employers.

The second layer is local law enforcement. And if you go out one ring from individuals and the private sector, you have 780,000 law enforcement officials across 18,000 state, local and tribal law enforcement agencies. Let me just say those numbers again: 780,000 across 18,000 departments. These men and women play an absolutely critical role, because they are the ones that can act on information they receive from individuals in the community, from their own observations, or from the intelligence community itself. But the ability of state and local officials, as well as the private sector, to prepare for threats and to respond to a disaster is only as good as their ability to receive useful information, understand what it means and act upon it effectively.

As Arizona governor, I took a lead role in creating our state's first law enforcement fusion center. Now, in a typical fusion center, an FBI agent might be sitting next to a state highway patrol officer; who might be sitting next to an Immigration and Customs Enforcement, or ICE, agent; who might be next to an agent from the DEA or from the tribal police. They don't merely share space. They share databases and techniques. They share ideas and experiences. They break down barriers and build networks.

This ensures that local law enforcement has better information necessary to protect our people, our neighborhoods, our infrastructure. Fusion centers are and will be a critical part of our nation's homeland security capabilities. I intend to make them a top priority for this department to support them, build them, improve them and work with them.

We've now moved three dozen intelligence analysts out to the field. In other words, as we build the fusion centers, we need to move analytic capacity from the Beltway to the country. So let's—how this is used. And I'll take it out of the terrorism context for just a moment. That if a law enforcement agency reports an increase in drug seizures of a particular type, that is a data point. That's a piece of intelligence. But a whole range of agencies working together in a particular fusion center can analyze that trend to understand what it means, how it will affect particular neighborhoods, and whether it foretells something even larger on the horizon.

In addition to the 70 current fusion center sites, the department will be collaborating with the Department of Justice and the FBI in more than 100 joint terrorism task forces across the country as well. So you see how we're creating the network—individuals, private sector, now among fusion centers and the law enforcement community.

Then we move on to the federal role. Since 2001, the United States government has invested considerably in reorganizing itself to counter the threat of terrorism. Now, DHS obviously plays the critical role here because we were given the explicit mission to secure our country against attack. So we, therefore, have an obligation to be clear about that mission.

We are not the FBI and we are not the CIA, but we need to work in close coordination with them and with all agencies who have part of the counterterrorism portfolio. And the way we are doing that is taking information shared amongst the Beltway and improving the sharing of information up and down the ladder—state, local, tribal communities—to the private sector. So the addition of the ability to share intel is the value-added that the Department of Homeland security provides.

And we also provide protection at our ports. CBP —Customs and Border Protection —is handling now security at 327 ports of entry.

The Coast Guard is patrolling 95,000 miles of American coastline.

But their roles all depend, and their effectiveness all depends, on the smooth flow of information and intelligence so that their actions are pivoted from data, from actual information. So as we improve intelligence-sharing among federal agencies, and that, in turn, with our own department components, we also improve intelligence-sharing with, as I said, state and local tribal partners.

Next, our international partners. At the widest level, we have the many players and partnerships that exist internationally, as well as more that need to be created. I mentioned earlier traveling 30,000 miles in the last few weeks. But here's what that's really about. DHS, together with the Department of Justice, State and others, is brokering agreements with our allies in Europe and around the world to share information on air travelers in advance of their travel, to gather critical biometric information so we know who is in our country, to scan baggage and cargo effectively while still facilitating legal trade and commerce.

The idea here—to paraphrase former Secretary Ridge—is that our physical United States border should be our last line of defense, not our first. So together with the Department of Justice, we have now forged agreements to prevent and combat serious crime with 13 international partners. There's more to do on this front.

Now, I want to give you a window into how important these partnerships are. Let me show you one example of our new approach and new thinking. Our growing relationship with Mexico is, of course, part of a broader effort, and it is designed to interdict not only the smuggling of narcotics, weapons, bulk cash and people at the United States-Mexico border but also designed to recognize our strong national, our homeland interests in the United States and Mexico and its relationship, and the whole national interest we have in making sure that Mexico and the crime there and the large cartels there are broken up.

This direct, interactive approach with our international partners is a new approach which we think is critical to dealing with things like cartel violence and also helps us ensure that that violence does not spill across our border or weaken Mexico's ability to be a strong partner with the United States.

So we're going well beyond what we've done in the past; for example, by inspecting southbound train cargo, cars and trucks, and in

fact, helping Mexico create an effective customs operation on our common southwest border that previously did not exist.

Let me close by going back to something I said earlier about people, because in the end, what we really do is about people. We are a nation of more than 300 million. More than that, we're a nation of families, communities, organizations, of cities, suburbs, tribes, all of their local governments and organizations. And within these groupings lies an extraordinary pool of talent, ingenuity and strength.

We face a networked enemy. We must meet it with a networked response. The job of securing our nation against the threat of terrorism is a large one, and it may never be totally completed, but we have a much larger chance at success if we strengthen our own networks by enlisting the talents and energies of Americans.

Countering the terrorist threat is not just the effort of one agency; it is one—or one element of society. Nor is countering terrorism the consequence of one tactic. Rather, it requires a holistic, unrelenting approach at all levels, with all tactics and all elements of society.

We need to be the very best at what we do, and that means engaging and empowering our citizens to be part of our collective effort, an effort aimed at effective prevention and of resilient response. So when I hear the phrase "Department of Homeland Security," I think of us as a hub, but the hub of a very large wheel that involves every single person in our country.

Thank you all very much. Here's the check.

Steiger: Thank you for a terrific and comprehensive look at the terrorism issue. And you've also reminded me that I haven't sent in my check yet—so I'll do that right away.

I want to give the members as much of an opportunity to have at you, but I can't resist asking you a couple of questions myself.

Aretha Franklin was one of many to note that every chain has got a weak link.

And when you—

Napolitano: I thought she sang about respect.

Steiger: Well, that too.

But as you seek to create this network of not just officials but individuals, how do you bring the less adept or less committed into the network, so that we've got across the country a —the kind of powerful, involved citizenry and officialdom that you're talking about?

Napolitano: Well, I think, one of the things we need to do is communicate that unfortunately the terrorist threat is not just focused on New York City or Washington, D.C., or a few other urban areas. Indeed if you look at the last couple of weeks, arrests have been made in places like Minneapolis and North Carolina.

So I think better education, about the breadth of the threat and how it can be carried out, is important. But even as we educate, we prepare. And again a lot of this preparation that I'm talking about has multiple uses, particularly in terms of response.

If you know or have planned with your family what you would do if an attack were to occur, that planning obviously has uses, should you have a tornado or a hurricane or other natural disasters. So education broadly but connected with also preparation and tools on, okay, well, how do you respond? Individual, family and then working with communities.

Steiger: You also alluded to the undeniable fact that terrorism can emanate from all kinds of places around the world and that intelligence is very important. The number of possible threats is infinite. So how do you zero in on the most important ones?

And yet the resistance of people, let's say, at the CIA—to share with the FBI and vice versa—is legendary. How are you doing, getting them to share with you, when they have a tough time sharing with each other?

Napolitano: Let's talk about that, because there has been a legacy of nonsharing in some respects, which is a luxury we can no longer afford.

And that is why we have a director of National Intelligence. In fact, our group, the principals—which means the head of the FBI, the head of CIA, myself, Admiral Blair—we will be meeting tomorrow. We regularly have luncheons, just ourselves, no staff, to make sure that we are effectively communicating the sharing of information.

I think the fact that I as the secretary of Homeland receive a daily intel brief—not just from members of the Department of Homeland Security, but also, for example, from a CIA briefer—helps make sure or ensure that critical intelligence is being shared. And in this administration we're very intent on exercising how we handle intel and how we respond. Indeed, right now there's a national-level exercise under way that will test some of this sharing capacity, whether things are being shared and whether responses are being correctly calibrated.

So, personal interaction, de facto interaction on a daily basis, and then exercising, I think, are the three major techniques to improve that intelligence-sharing environment.

Steiger: One more, quickly, and then I'll go to the members. Any learnings from the swine flu situation, which turned out to be much less bad than people feared?

Napolitano: Well, first of all, we're learning wash your hands—cough correctly.

But we have had, actually, over the summer a lot of work done on H1N1. Why? Because we anticipate it will be coming back this fall. It obviously focuses on a younger population than seasonal flu. We will not have vaccine available before the school year starts.

And so one of the things we are trying to prepare and network and are testing some of the ideas I just suggested about empowering individuals and communities really involves preparation for this fall and a return of the H1N1 in what could be—we don't know—science cannot yet tell us—but it could be a more severe form of the H1N1, because it mutates as it travels, than we saw last spring; so that was perhaps just a dress rehearsal.

One important thing, if I might add, is this—the H1N1 was a—during that outbreak, the president used an executive order known as HSPD 5 to designate the secretary of Homeland Security as the principal federal official. In other words, this was a — an event that crossed many different departments, agencies of the federal government—so really, for the first time using the Department of Homeland Security in a way I think it was originally intended, which was to be able to take not the lead operational role—obviously, particularly on something like this, HHS is the—has such a lead, important role—but to make sure things are properly coordinated and, importantly, communicated with the American people.

Steiger: Okay. I'd like to invite the audience to join. Remember a couple of things: wait for the microphone; stand; identify yourself; one question; no speeches.

The gentleman right here. Wait for the microphone.

Napolitano: It's right behind you.

Questioner: Hi, Paul.

Steiger: Hi.

Questioner: Secretary, I was very admiring of your comments. But as I sat there, I heard you speak several times about what our citizens need to—how we need to implicate our citizens in more efforts. Are you suggesting we need train our people from school days on to be more alert and watch more carefully their school people, their schoolmates, their workers, their family, their neighbors, and then to more effectively report what they see to some authority?

Napolitano: You know, I think there's actually an important role that we can play in educating even our very young about watching for and knowing what to do if—if you're in an airport and you see a package left with no one around; you know, that sort of thing. I also think we could do a much better job at educating young people about how to—how to prepare how to handle themselves so that they can protect themselves also if something untoward were to happen.

So do we have a plan in that—in that way, or have we actually worked that angle of this? Not yet. But I think you're getting the gist of what I'm saying, which is to say we need a culture of collective responsibility, a culture where every individual understands his or her role; which goes along with my saying that the more we prepare, not only the stronger we are, but the more preparation you have, the less fear that you possess.

Steiger: Right here. Here it comes.

Questioner: Thank you. Paula DiPerna, Chicago Climate Exchange. Thank you for your remarks.

I want to just drill down (sic) a little bit on something you said about infrastructure, that 85 percent of the infrastructure is privately managed. And for—the question has to do with, to what extent can you interact with the private sector when they, for example, lay off people and those layoffs have direct implications on protecting the public?

For example, very small example, pay phones in New York City practically don't exist. At 9/11, the only phones that worked were pay phones. Those are the only things that people could use to communicate, and cell phones are highly incompatible. So how would you broker that? You know, there's a—there's a financial incentive to eliminate pay phones; Homeland Security needs them.

Napolitano: I think in those types of—and I want to—situation—what you do is you —and we are doing and have been doing—is you say, all right, you don't want to continue that anymore. What is your plan for how people can be—communicate with each other in the type of disaster that may occur?

And the point here, again, is—and it really points out how technology has changed and is changing rapidly. And the more we work together, we can share ideas about, okay, well, then, how do you use different types of technology in a communications environment where the pay phone may be obsolete? Because I think we have to assume that, you know, pay phones are not only obsolete in New York but they're pretty much obsolete across the country. They're going the way of the record album and other things of our youth.

Steiger: Way back there by the post.

Questioner: Hi. I'm Bill Drozdiak. Madame Secretary, given what you've learned on the job over the past six months, both about the nature and magnitude of the threat and whatever abuses may have occurred in the previous administration, do you think that the laws governing domestic surveillance need to be changed in any way?

Napolitano: I think that, to the extent domestic surveillance is being carried out, it's as much an implication of operations as of legal authority. It's more de facto than de jure, if I can use those phrases. And we have to be careful.

And let me make an important point here, so I'm glad you asked that question. Because as I discuss a culture of awareness, individual preparedness, the ability to identify suspicious activities and the like, there's a careful balance to be struck between that and a feeling like we're trying to create a culture of everybody spying on one another. And that's a balance to be struck, and it's an important one that we all discuss collectively. We don't want that. But what we do want is something that helps provide for our collective safety. And that is something that we all need to be conscious of.

And we build into and are building into the things we are doing not only consultation about constitutional and civil liberties aspects of what we're doing through -- we actually have now a whole department on that -- but we also look at issues about privacy and protection of personal privacy, and how those concepts and principles can also be incorporated, even as we build a culture of collective awareness and preparation.

Steiger: Ma'am, back there. Yes, you.

Questioner: We were delighted when you were appointed DHS secretary, and we're disappointed with the expansion of enforcement mechanisms that continued the Bushisms of the past, particularly around immigration. We've got a broken immigration system, yet DHS has expanded 287(g). Secure Communities is doing anything but making people secure. Racial profiling continues to be a very big problem in this country. And in your remarks around protecting against terrorism, we didn't hear very much about protections against racial profiling or the restoration of due process and fairness into systems that actually protect individual citizens, permanent residents and other people who live in the United States. We'd really like to hear your thinking about why you're expanding enforcement without fixing a broken immigration system.

Steiger: Could—I'm sorry. I —could you—

Questioner: My name is Mallika Dutt, and I'm with Breakthrough.

Napolitano: Well, first of all, we are expanding enforcement, but I think in the right way. We have, for example, revisited the whole issue of work site enforcement, the focus on employers.

The program you reference many in the audience may not know. We shorthanded it 287(g), which was created during the Clinton administration, which allows state and local law enforcement to have a memo of understanding with the federal government to have some immigration authority. Otherwise, it's exclusively federal.

But we did that because the previous MOUs with local law enforcement really had no standard accountabilities or even terms built into them. And so rather than just continue with these MOAs that were very vague and didn't allow us to prioritize within 287(g), we said no, we're going to redo all of them.

When we do that, we'll expand to some other communities, although not all that have requested them. But that will give us some authority to really focus on two groups: one, those who are already incarcerated, so we don't have the system where somebody breaks a criminal law, they're handled in the criminal system and then released into the public, and then ICE or whatever other— Immigration has to go out and find them, which uses an extraordinary amount of resources; and two, really looking for gangs and also criminal fugitives who happen to be in the country illegally.

Our MOA's are written to focus on those groups.

Secure communities, what that is, is a way to have the immigration database right in prisons and the like and to train correction officers on how to use them properly, so that as people finish their sentences, the deportation process, the removal process, can be done smoothly.

I started this, when I was the governor of Arizona, out of the Arizona prison system. And it's a very effective way, as a force multiplier, to really make sure that those types of immigrants that have already broken our criminal laws, and these are criminal laws in addition to immigration laws, go into the removal process. You may disagree with that as an enforcement strategy. I think it's the

right way to target, a strong enforcement strategy.

Now, on the overall immigration law, I agree with you. I believe that we need to look at the whole package. And that obviously I cannot do by myself. The Congress has to do it.

Now, I was with the president when he met with 30 congressional leaders—both parties, both houses—and said he would like to move something through at the end of this year, the beginning of next year. And I'm heavily involved in those efforts, as is your senator from New York, Senator Schumer.

And we need to work together, to really look at why bills didn't pass in the past, how we build even stronger enforcement into immigration reform. But we need many other things as well. And I would very much respect your ideas in that regard.

Steiger: Right here, please.

Questioner: Annette Gordon-Reed.

You began speaking about developing rules, against terrorism and fighting terrorism, that are consistent with values. Are there any problems, do you see, with developing a notion of citizens who have a collective responsibility to report on one another?

I mean, where's the balance between sort of the individual sort of accepting people, in your community, and at the same time being little private attorney generals?

Napolitano: Yeah, that's the point I was making a bit earlier, about being very sensitive to that. And that's where education really can come in. What is something that should be reported? What isn't? And there are materials from a variety of aspects that help with that kind of education. And so really the first questioner said, what are you doing to educate young people about that? I think that's where it has to start.

Steiger: Right here.

Questioner: Kenneth Bialkin with Skadden, Arps. My question bears on the same delicate civil liberties issues that you've already delved into, and I know it's hard.

Every profile that the press reports on terrorists, domestic terrorists, suggests that they made their contacts and had their activities in their mosques, that it is in the mosques where the -- where they meet and plan and work. And obviously surveillance and education has to bear on what might be done in terms of educating those societies and alerting those people to the risks that their communities and others face.

Is that responsibility one which resides in your department? Is it shared? And what can you say about that particular focus, when we know that so much happens in such a restricted area?

Napolitano: Well, a couple of things. The direct answer to your question is that sort of activity is primarily the domain of the FBI.

But I think we have to be very careful about profiling a religious institution just as we have to be careful about profiling individuals. And that's why how you develop intelligence that's actionable needs to be very carefully done and not restricted or done in that religious environment.

Where we can help in our approach is to work with leaders in a variety of faith-based communities not just on education but really to have good community outreach, so if they perceive that there is something going on that is aimed at violent extremism or an extremist attack, they feel comfortable working with law enforcement in advance of that attack occurring. But I think we have to be very, very careful about interfering with the free exercise of religion or profiling in that sense.

Steiger: Right there. Yes.

Questioner: Bal Das from Kailix Advisors. Madame Secretary, in the network response, you identified a key component, which is greater international cooperation. And at the beginning also you laid that out as being one of the framework of an effective response, since your borders—since our borders are the last, rather than the first, response.

How closely do you work with the State Department, in terms of the projection of American soft power as compared to hard power being at the nub of winning of the hearts and mind, which goes a great distance in making sure that the inspector in Karachi is not just obligated by a bilateral shared security treaty but genuinely feels that he needs to ferret out more information and share with a nation whose value system he or she empathizes with, whether it's Karachi or New Delhi? So I wonder how—I would appreciate your thought on how closely you work with the State Department and in the projection of American soft power as—about your strategic thinking. Thank you.

Napolitano: Yes. We work, obviously, very closely with the State Department in the international environment. Indeed, when I travel

internationally, I immediately link up with whatever embassy or consulate is where I'm going, so that we attend and go to things together. So when I met with, for example, the president of Pakistan a couple of weeks ago, the ambassador was with me. Why? Because we want to show that we are linked together and have a common message and in—to use that as an example as an area where we can assist in helping create a civilian law-enforcement presence that would take the place of a military presence, particularly in certain parts of the country.

Perhaps a more direct example is Mexico, where Congress actually appropriated —it's called the Merida Initiative—to be used in conjunction with the federal government of Mexico to buy equipment and, importantly, to train civilian law enforcement.

And I want to just pause a moment on this. Our ability as a nation to work with other countries on having a—not just a law enforcement but justice systems that are civilian in nature as opposed to military, I think, is very, very important.

And that's one of the things that we have expertise in within the Department of Homeland Security, particularly when you're talking, for example, about how do you set up a port of entry, you know? How do you run it? What does it look like? What kinds of technology should be employed? What works? What have we found that doesn't work? What kind of training needs to be—needs do you need to have? What kind of supervision do you need to have? How do you prevent corruption from occurring or from infiltrating the ranks?

How do you create public trust that the people who are running ports are not simply on the dole and you can just pay them off and any kind of contraband can go through? So that transition from military to civilian, I believe, is where our department can play a key role.

Steiger: One or two more. Steve?

Questioner: Secretary Napolitano, Steve Flynn, with the Council on Foreign Relations. Thank you again for coming here today and sharing such an important address with all of us. And also, thank you for doing the —what arguably is Washington's, I think, most challenging job.

Adding to that challenge —let me ask this. As we know, basically, with safety or something like making a home handicap-accessible, the best opportunity to put things like security resilience into a system is in the design or the start-up phase. The president is engaged in commitment to invest in our infrastructure, revise our health-care system and a host of other important imperatives for rebuilding our country. To what extent is your voice on the security resilience issues able to be a part of those important endeavors? And can we get it right in the early phase, instead of coming in, trying to paste it on afterwards?

Napolitano: Right. Absolutely, we can get it right.

And let me give you an example of that, Steve. In the stimulus money, that which is coming to the Department of Homeland Security is being used, for example, to purchase technology in airports that we think will increase our overall security capacity. At the same time while the technology is being built and the space for the technology is being built, you have a job-creation stimulus at the same time.

Another example, which may not be as self-evident, is the money that went to the Department of Transportation. Now, they got a lot of money to build roads and bridges and other things to put Americans back to work, but there are ways or design features that can be incorporated that enhance safety and security at the get-go rather than having to pick up the pieces at the end of an event.

So there is a close intersection or interaction now between our —folks at our department who specialize in critical infrastructure like that and the Department of Transportation on what should be looked at in those construction projects as we move forward.

Steiger: Madame Secretary, on behalf of the council, I want to thank you for a very comprehensive discussion.

Napolitano: Thank you all. Thank you.

Thank you, Paul.

Steiger: Thanks a lot.

###

This page was last reviewed/modified on July 29, 2009.