Remarks by Secretary Napolitano at the Interagency Council for Applied Homeland Security Technology's Counter-IED Symposium

Release Date: December 1, 2009

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

Secretary Janet Napolitano: Thank you all very much. It's a pleasure to be here. I must say I think it's my first time out at this particular venue, and I'm glad to see it. I have not yet gone into the ice sculpture room yet. Have you seen that? Do you know what I'm talking about? Okay. But in any event, thanks for the welcome. And I'd like to thank the Interagency Council for Applied Homeland Security Technology [ICAHST] for inviting me to speak today.

I was joking the other day that the homeland security arena has a lot of acronyms, and they seem to be multiplying and getting longer each day. But I think when we add it all together—NCCIC, which is the National Cybersecurity Communications Integration Center, when we have ICAHST, et cetera, et cetera—what we basically are saying is we have a lot of very intelligent people working on a number of difficult security challenges facing our country.

So today I want to recognize our many federal, state, tribal and local partners who have come together to speak about and talk about one of the most serious threats to the homeland—the threat of an attack via an improvised explosive device [IED].

Now, we all know that IEDs come in many forms, and that building them does not require a lot of technical sophistication or materials—that they can be used and have been used on land, sea, or in the air. And as we know all too well, they can cause extensive damage and loss of life as well as chaos and disorder.

So this is a threat that we take most seriously at DHS [Department of Homeland Security], and as I know everyone in this room does. And it is a threat that the Obama administration is fully committed to protecting against, whether here at home or overseas, in support of our nation's military and our own allies. Simply put, the IED threat warrants our sustained attention as well as our best thinking.

The recent arrest and indictment of Najibullah Zazi on a charge of conspiracy to use weapons of mass destruction—in this case, with explosive bombs—against persons or property in the U.S. serves as a vivid example of the kind of threat we continue to face.

And because this threat ties directly to events in the Afghanistan/Pakistan theater, we must continue to put additional pressure on al Qaeda and ultimately diminish the threat that they pose to the United States and to the international community—a plan that the President will detail in his strategy this evening when he addresses the nation about Afghanistan and Pakistan.

So today I want to talk with you about what we can do collectively and individually to protect against the threat of IEDs right here at home.

I want to talk about the kind of public-private partnerships, technology, information sharing and public education that I believe are necessary at all levels to achieve our aims. And I want to talk about how our efforts fit into a larger but no less significant challenge, which is protecting our nation's critical infrastructure from a range of threats, whether from terrorist attack, natural disaster, cyber attack, or infectious disease.

So I know that over the next three days, you will delve into many of the technical and organizational aspects of this difficult issue. But let's step back just a bit and talk about IEDs as one very serious threat among a range of threats we face from terrorism and radical extremism. I also want to address how this threat fits within the great need we have to secure the nation's critical infrastructure.

Now, there are often a lot of "terms of art" and jargon used in this field, but we shouldn't necessarily assume that everyone is comfortable with all of it. So let's speak in simple terms about what is at stake.

We have all seen the horrible toll explosive devices have taken in battle in places like Iraq and Afghanistan. We've witnessed the terror of Oklahoma City, the Madrid and London bombings—to name just a few incidents. But beyond the human, economic and psychological toll of these horrific events is the effect such attacks can have on our critical infrastructure.

Critical infrastructure is defined as something our society depends upon such that if it were damaged or destroyed, it would have a significant impact on our ability to function.

So let me repeat that—critical infrastructure is defined as something our society depends upon such that if it were damaged or

destroyed, it would have a significant impact on our ability to function.

Think of the nation's power grid or banking system. The Internet. Water treatment facilities. Nuclear power plants. Transportation. Our food supply chain and agriculture.

A terrorist attack—or even a natural disaster like a hurricane or earthquake, against or in the vicinity of any of these things—can significantly disrupt the functioning of the government, the private sector, and produce cascading effects that go far beyond the physical location of the particular incident.

Accordingly, we all have a stake in the protection of these vital assets and key resources. It follows, then that all of us have a role and responsibility to do our part in ensuring their resilience. And everyone has a role to play—government, private sector, nonprofits, communities, individuals.

At DHS, we have been saying again and again that making our nation more secure and more resilient is a shared responsibility. No one government department can do it all.

As individuals, we need to exercise a greater sense of vigilance, to say something if we see something, and a stronger commitment to the preparedness of our families, communities, and businesses. This means all of us having an awareness of what to look out for, of how to spot suspicious packages or individuals, of whom to call in emergencies.

These are not hypotheticals. Attentiveness by store clerks has led to bomb plots being foiled. Vigilance by border guards has kept bomb-making materials out of the United States and put those who sought to bring them in jail.

Now, let me talk about the Department's exact role. As members of government, we have a major role to play in making our nation more ready and resilient. Indeed, this is the central mission of the Department of Homeland Security. But at DHS, we also know that we are not "the team." We are part of the team. And our private sector—in whose hands the vast majority of the nation's critical infrastructure rests—must play an absolutely critical role as well.

This means that government and industry, as well as the many small businesses who may have connections to the 18 critical infrastructure sectors, must work together to build trust and learn from each other.

Here is an example: DHS has in the past, and will be again next week, worked with officials from the hotel and retail industries on strategies for getting frontline workers some basic training on spotting suspicious behavior. This is precisely the kind of training that has helped us disrupt threats in the past.

Threats to critical infrastructure: these partnerships are critical, given what we know about the current threat environment. Now, as you know, the consensus view of the intelligence community is that the terror threat to the homeland is persistent and evolving.

The recent FBI [Federal Bureau of Investigations] arrests of terror suspects in the United States further underscores that al Qaeda, its affiliates and those inspired by its ideology intend to attack us here at home. We must adapt quickly to new and emerging threats such as cyber crimes, attacks on critical infrastructure, and the rapid spread of pandemic disease.

Now, this administration has been forceful about engaging the whole range of threats using all the diplomatic, military, economic, technological, educational and cultural tools at our disposal.

But to ensure a streamlined and complimentary approach to threats, we have partners—and we've partners with the Department of Justice and other agencies—to develop important national-level planning documents, including the national strategy for combating terrorist use of explosives in the United States, as required by Homeland Security Presidential Directive 19.

At DHS, the Office for Bombing Prevention is responsible for coordinating this participation. And under the HSP-19 framework, DOJ, DHS, Department of Defense, and other partners have created a joint program office to lead and coordinate the execution of policy and programs to combat the terrorist use of explosives in the United States.

Our goal is to create a national framework focused on five key areas to combat the IED threat: prevention, detection, protection, response, and research and development. In each of these key areas, we coordinate with state and local partners, especially those with specialized responsibilities such as bomb squads, dive teams, and explosives detection canine squads. Let me go through each five.

Prevention: our first task is to focus on prevention, and that starts with providing tools and resources to our state and local partners to build capabilities and countermeasures to reduce our overall risk. The $1.7 billion homeland security, transportation security, and infrastructure protection grant programs are a primary means for building our prevention capacity. For the past two years, counter-IED capabilities have been highlighted as priorities in these homeland security grant program guidance documents.

Another key to prevention is information sharing. Our Office of Bombing Prevention developed and launched the technical resource for incident prevention know as the TRIPwire—a secure information-sharing portal to provide intelligence and analysis on terrorist IED tactics, techniques, and procedures—and to provide those to qualified officials and law enforcement authorities. TRIPwire is currently used by over 8,000 users

currently used by over 6,000 users.

To address the need of the private sector for access, to focus information, we created a similar portal tailored to the private sector called TRIPwire Community Gateway. So you have TRIPwire for law enforcement; for the private sector, you have TRIPwire Community Gateway.

We also are sharing information with the public and suppliers of precursor chemicals so that they can be better informed and prepared. And we are educating private sector suppliers and employees, through our Bomb-Making Materials Awareness Program, to help them identify the materials used to build IEDs. Acting Under Secretary Bart Johnson will be here later on Wednesday to address some of these and other activities in which the Department is engaged—to better share information and intelligence with our state and local partners so that they can better assist us in the prevention factor of our work.

Detection: we are working to increase our detection capabilities by expanding our explosives detection technology in several ways. For example, TSA [Transportation Security Administration] has deployed over 1,500 explosives detection systems and 7,500 explosives trace detection machines at airports across the country to screen checked and carry-on baggage.

TSA has also established the Bomb Appraisal Officer program at over 100 airports to increase the accuracy and efficiency of screening operations and IED detection. With the Screening of Passengers by Observation Techniques—SPOT—program, TSA officers are focusing on passenger behavior for signs of malicious intent.

And we also have approximately 700 explosives detection canine teams deployed throughout the country—providing an increased layer of security at airports, mass transit systems, border crossings, and federal buildings.

Third, protection: a significant part of our protection effort centers on critical infrastructure, as I've mentioned before. The National Infrastructure Protection Plan, the NIPP, lays out the partnership approach, and the Government and Sector Coordinating Councils work together to develop priorities for government and the private sector to protect our critical infrastructure across the 18 critical infrastructure sectors.

Our Office of Infrastructure Protection has deployed over 90 protection security advisors throughout the nation. They in turn have supported state and local responders, and owners or operators of critical infrastructure, by coordinating protection efforts including planning, training, assessment and incident management support.

The Office of Infrastructure Protection has developed more than 2,000 buffer-zone protection plans to extent terrorism prevention and protection efforts, including those for IEDS, into the communities that surround our most important infrastructure sites.

So you have the 18 sectors, and they in turn have developed 2,000 buffer zones, all of which now have approved plans.

Of course, we want to reduce the risk posed by the use of dangerous chemicals in IEDs or other attacks, and ensure that we protect the chemical facilities themselves. And we're doing that through the Chemical Facilities Antiterrorism Standards—CFATS. And those rules now are out, and they're being implemented right now for the larger or Tier 1 and Tier 2 facilities.

The Office of Infrastructure Protection is also responsible for enforcing CFATS, among its other obligations, and we are in the process of establishing the workforce necessary to inspect facilities and work with owners and operators throughout the country.

Fourth, response: to strengthen our response in a potential attack, we have focused on response planning, capabilities analysis, and planning across jurisdictions. Specifically, we have conducted onsite response capability assessments for over 175 state and local bomb squads and dive teams. This has given us a better understanding of the nation's overall preparedness, and we will guide it and use it to guide future investments and track current progress.

Fifth, research and development: finally, and perhaps most significantly, our Science & Technology Directorate has established a counter-IED program to focus our nation's research, development, testing, and evaluation community on reducing the risk of an IED attack.

I know that Ruth Dougherty, the program executive officer for counter-IED, has already discussed some of our specific efforts. But the range of technologies supported by our Science & Technology Directorate is aimed at early detection and effective response, and that is with respect to multiple types of IEDs—some that have already been deployed, some that are only deployed in our imaginations. But we always have to be working to think ahead of the terrorists.

I would like to close by saying that at the end of the day, our success will hinge on our ability to work with our partners across the board at all levels of government and the private sector to monitor, protect against, and ultimately reduce the threat of an IED being used successfully. Our engagement with ICAHST is a good model for the kind of partnership that we seek to have.

I wish you a successful symposium. Thank you for the work that you are doing to keep our nation secure. And I would like to thank you—not just for what you have done, but for the work you are about to do.

Thank you very much.

###

This page was last reviewed/modified on December 1, 2009.