THE HONORABLE JANE HARMAN
TESTIMONY
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
SEPTEMBER 11, 2013

Twelve years ago today, as the towers were falling and the Pentagon fire was burning, I was walking toward the US Capitol. My destination was the intelligence committee rooms in the Capitol dome—the place most believe was the intended target of the fourth plane which, thanks to the heroism of its passengers, went down in Shanksville, Pennsylvania. My staff called to alert me that the Capitol had just been closed, as were the House office buildings. So most of Congress and I milled around on the lawn in front of the Capitol. There was no evacuation plan. We had no roadmap for a response.

Part of the solution which some of us in the intelligence and counterterror field recommended was to create a dedicated homeland security function. The White House proposed a much more ambitious concept, and in order to pass legislation to create this new capability, Congress agreed to combine 22 agencies into the Department of Homeland Security (DHS).

Now in its tenth year, I'm proud of my role as one of the Department's "founding mothers" and want to thank the thousands of DHS employees serving us daily around the country and the world. As I speak, Customs and Border Patrol (CBP) agents in mega-ports like the port of Dubai are screening US-bound cargo for dangerous weapons and materials, specially trained Homeland Security Investigation agents in diplomatic posts around the world are reviewing suspicious visas, and TSA screeners are daily depriving al Qaeda and other terror groups the ability to turn more aircraft into weapons – a tactic we know they continue to attempt.

Today, DHS remains a work in progress but the efforts of its people are its backbone. And ours.

I testified before this Committee last year, and said that there are homeland functions that work well, including:

- CBP and TSA efforts to prevent suspicious individuals from departing foreign and domestic airports while allowing the rest of the flying public to travel,
- Expansion of the See Something Say Something campaign,
- Coordination with state and local law enforcement, including fusion centers, to identify terror suspects, and
- A massive vulnerability assessment of US critical infrastructure.

But I noted challenges:

- The failure of the intelligence function to fully develop at DHS,
- The need for DHS to focus more on its relationships with critical infrastructure owners and operators (which is now happening), and
- The failure of Congress to reorganize its committee structure.

Since I testified, much has happened. There is good news and bad news.

The bad news first:

- we failed to thwart the Boston Marathon bombing,
- there has been an exponential increase in cyber attacks,
- another devastating Hurricane,
- Edward Snowden, and
- bombmaker Ibrahim al Asiri of al Qaeda in the Arabian Peninsula is still on the loose.

The significant good news is that we are doing better on four major fronts:

- information sharing,
- resilience,
- collaboration with the private sector on cyber, and
- we're getting ahead of privacy concerns.

Information Sharing

Information sharing since 9/11 has improved dramatically, but there is more to be done. In the past year, while we were not able to stop the Boston bombing, our sharing of information after the attack was better and faster than it has ever been. Boston PD worked seamlessly with local, state and federal intelligence and law enforcement agencies to identify the suspects and detain them, using extensive camera footage and cell phone data. This was the first full-scale effort to use the American people as a significant investigative resource.

DHS homeland security grant money was critical – according to the Boston PD – in making sure that the city was trained to share information rapidly during an emergency. DHS also participated in the Multi-Agency Coordination Center (MACC) that was operational before and during the marathon. Representatives from Boston's police, fire, and emergency medical services, as well as public safety personnel from seven other cities and towns along the marathon course participated. The MACC was a critical in coordinating communications once the bombs exploded.

Resilience

At the time of the bombings, Boston was one of the best-prepared cities in the country to handle an emergency event, in large part because of DHS's preparedness and resiliency programs and collaboration with state and local officials. Last fiscal year, DHS distributed almost $11 million to Boston through its Urban Areas Security Initiative (UASI).

That money had been used, in part to upgrade over 5,000 portable radios for first responders, install a communication system inside the tunnels of the Boston T, and to conduct two citywide disaster simulations in collaboration with DHS. Using the preparation and after-action reports from the first trial (in May 2011), local and state authorities worked to improve the city's preparedness in a second city-wide drill, in November 2012, less than a year before the bombings. Boston Police Commissioner Edward Davis has said that the "interoperability" learned during those drills "made a difference in our ability to respond to the Marathon."

DHS also responded successfully to Hurricane Sandy. On October 27th, FEMA activated its National Response Coordination Center, a multi-agency center based at headquarters in Washington. By October 28th, just before Sandy made landfall in New York and New Jersey, more than 1,032 FEMA personnel were positioned deployed along the East Coast working to support disaster preparedness and response operations, including search and rescue, situational awareness, communications and logistical support.

Collaboration with the Private Sector on Cyber

DHS will never "own" the cyber mission, but it is responsible for a central piece: critical infrastructure protection. In the past year, DHS has tracked and responded to nearly 200,000 cyber incidents – a 68% increase from the year before.

I have seen firsthand how the Department is working hard to build strong and lasting relationships with the private sector – owners and operators of critical infrastructure – and the IT companies that help those facilities function. In June, the Wilson Center hosted Secretary Napolitano for an off-the-record discussion between industry and the Department about what's going right and what's going wrong.

We heard that real-time data sharing about threats will be hard, but if industry knows their counterparts at DHS who can then coordinate with other government agencies, the process is a lot easier: they can just pick up the phone. The National Cybersecurity and Communications Integration Center (NCCIC), now open now about four years, has responded to almost half-a-million incident reports and released tens of thousands of actionable alerts to the public and private sector partners. In the same room, DHS has different government representatives from different government agencies all talking together – with the private sector. This is unheard of.

The Secretary spoke publicly about how important this mission is for DHS, calling it a "grand experiment," – the first time that our government has approached a major national security problem hand-in-hand with the private sector.

Getting ahead of privacy concerns

Recent disclosures by Edward Snowden have shown that in most cases, our self-policing system works. But privacy and civil liberties concerns will only grow as our government becomes more intertwined in the cyber experiment.

At DHS, there is a privacy and a civil liberties office mandated to review – on the front end – DHS policies to make sure there are appropriate protections for personal private information built in from the start. Regular "Privacy Impact Assessments" are issued for any new or substantially revised information technology system within the Department, and the DHS Civil Rights and Civil Liberties Office has delivered training to Privacy Officials at 68 of the 78 fusion centers.

In-house efforts at DHS should finally be augmented by the Privacy and Civil Liberties Oversight Board, which became operational in May of this year – 9 years after it was established by the 2004 intelligence reform law.

DHS will continue to face difficult challenges going forward, including al Qaeda's enormous ability to evolve, the rise of lone wolf terrorists, the constant increase in type and sophistication of cyber attacks – especially the risk of exploits in software, and privacy issues related to information technology.

To return to my introductory remarks, thousands of selfless DHS people deserve our thanks. So does former Secretary Janet Napolitano for her service over the last five rugged years.