Opening Statement of
Senator Susan M. Collins

Anticipating Evolving and Emerging Threats

Committee on Homeland Security and Governmental Affairs

July 11, 2012

★ ★ ★

The terrorist threats facing our country have evolved since the horrific attacks on 9/11. That awful day steeled our national resolve and drove us to rethink how our intelligence agencies were organized and how our instruments of national power ought to be used.

Since then, we have taken significant actions to better counter the terrorist threat, but the terrorists have constantly modified their tactics in an attempt to defeat the security measures we have put in place. The October 2010 air cargo plot involving explosives hidden in ink cartridges shipped from Yemen is just one example. The bomb-makers from Al Qaeda in the Arabian Peninsula apparently sought to avoid improvements in passenger and baggage screening by exploiting vulnerabilities in cargo security.

Let me emphasize that it is extremely troubling that terrorists have been aided in their efforts to circumvent our security by the all-too-frequent leaks regarding our counter-terrorism activities and capabilities. As we consider the challenges posed by emerging threats, we cannot tolerate giving our adversaries information they can turn against us.

When Chairman Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our goal was to create a coordinated effort among the Department of Homeland Security, the Director of National Intelligence, and the National Counterterrorism Center, as well as other federal partners and stakeholders.

One instrument used in these collaborative efforts has been the network of 77 state and local fusion centers that help manage the vital flow of information and intelligence across all levels of government. These centers are recipients of national intelligence products, but must also become robust aggregators and analyzers of information from their own areas that can be shared so that trends can be identified and the understanding of threats in our homeland can be strengthened.

An example of the effectiveness of fusion centers occurred on June 25th, 2011, when the Colorado State Patrol attempted to pull over a man driving erratically, who fled authorities and eventually crashed. As the police processed the driver and information about his pickup truck, they learned from the Colorado fusion center that he was linked to an attempted bombing of a bookstore. The driver is now in custody facing federal charges.

This type of grassroots teamwork is essential to combat a deceptive and often elusive enemy. As discussed in a recent report by the Homeland Security Policy Institute at George Washington University, however, fusion centers have yet to achieve their full potential.

Questions have been raised about their analytic capabilities and about whether they duplicate the work of the Joint Terrorism Task Forces.

The reforms enacted in response to the 9/11 attacks have helped to ensure that there have been no other large-scale attacks in the U. S. The absence of such attacks in the U. S. and our success in thwarting terrorist plots should not lull us into a false sense of security – for this is no time to rest, as gaps in our security net remain.

We continue to witness the growing threat of violent Islamist extremists within our borders. Sometimes these terrorists have been trained overseas; others have taken inspiration from charismatic terrorists via the Internet – plotting attacks as lone-wolves.

Last year, as members of this committee well know, two alleged Al Qaeda terrorists were arrested in Bowling Green, Kentucky. This highlighted a gap where elements of our security establishment had critical fingerprint information that was not shared with those granting these men access to our country.

Another growing and pervasive threat is that of cyber-attacks. Earlier this year, the FBI Director Robert Mueller warned that the cyber threat will soon equal or surpass the threat from terrorism. Just last month, several former national security officials wrote that the "cyber threat… is imminent, and that it represents one of the most serious challenges to our national security since the onset of the nuclear age sixty years ago." They further wrote that "protection of our critical infrastructure is essential in order to effectively protect our national and economic security from the growing cyber threat."

Chairman Lieberman and I have been working with our colleagues on legislation to address the cyber threat to our nation's most critical infrastructure, such as the power grid, nuclear facilities, water treatment plants, pipelines, and the transportation system. I can think of no other area where the threat is greater and we've done less.

There is also the growing threat from Transnational Organized Crime. Director of National Intelligence James Clapper has testified that transnational criminal organizations, particularly those from Latin America, are an "abiding threat to US economic and national security interests." Our intelligence community needs to focus on their evolution and potential to develop ties with terrorists and rouge states.

The 9/11 Commission devoted substantial attention to the challenge of "institutionalizing imagination." In an understatement, the Commission's report observed that, "[i]magination is not a gift usually associated with bureaucracies." Yet, imagination is precisely what is needed to address emerging threats. We must persistently ask: Where are the future threats? What technology could be used? Do we have the intelligence that we need? Are we prepared to thwart novel plans of attack? What will our enemy look like in two, five, or even ten years?

Surely we are safer than we were a decade ago, but we must be relentless in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden has proved, America's resolve and creativity are our most powerful weapons against those who seek to destroy our way of life.