Opening Statement of
Senator Susan M. Collins
"Homeland Threats and Agency Responses"
Committee on Homeland Security and Governmental Affairs
September 19, 2012
★ ★ ★

Last week, we observed the eleventh anniversary of the horrific attacks of September 11th, 2001. We again remembered the victims and heroes of that day. And we acknowledged the dedicated military, intelligence, law enforcement, and homeland security professionals who have worked together to bring terrorists to justice and to prevent another large-scale attack inside the United States.

Tragically, however, we have also witnessed violent attacks on the U.S. Consulate in Benghazi, Libya, the resulted in the killings of our Ambassador and three other brave Americans. While these attacks remain under investigation, it is difficult not to see shades of the 1998 attacks on our embassies in Kenya and Tanzania, which were among the many precursors to the attacks of 9/11. This tragedy underscores the ongoing threat we face, both abroad and at home, from violent Islamist extremists.

In the aftermath of 9/11, we took significant actions to address this threat. When Senator Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our aim was to improve coordination within the Intelligence Community and among the key stakeholders at all levels of government. Achieving the goals of this landmark law remains a work in progress.

We know we face a determined enemy. Al-Qaeda in the Arabian Peninsula (AQAP) has tried repeatedly to exploit holes in our security. The failed 2009 Christmas Day bomber used a device specifically designed to avoid detection. The 2010 cargo plot sought to circumvent improvements in passenger screening by targeting cargo. In May of this year, al-Qaeda tried again. The bomb-maker apparently sought to avoid the failures of the earlier Christmas Day attack. Through the aggressive efforts of our intelligence community, this plot was disrupted before it could threaten American lives. Nevertheless, that operation was also plagued by leaks – apparently from within the Executive branch – that may have undermined future efforts.

Not every threat that we face has been met with sufficient resolve and action. Perhaps the best example is the ever-increasing cyber threat. Experts have repeatedly warned that the computer systems that run our electric grids, water plants, financial networks, and transportation systems are vulnerable to a cyber attack that could harm millions of Americans.

Just last week, former Deputy Secretary of Defense John Hamre said that the threats in cyberspace "took a darker turn" this summer, as three very large corporations experienced cyber

attacks “designed to damage operations.” Citing government sources, he said that at least two of the attacks may have come from Iran. China and Russia have also launched cyber attacks.

To respond to this escalating threat, the Chairman and I have worked during the past two years to craft a bipartisan bill that relies on the expertise of government and the innovation of the private sector. Despite our hard work to find common ground, the Senate has failed to pass cybersecurity legislation. Given the significant damage already done to our economy and our security, as well as our clear vulnerability to even worse attacks, this failure to act is inexcusable.

Former DHS Secretary Michael Chertoff and former NSA and CIA chief Michael Hayden describe the urgency this way: "We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9/11' hits - it is not a question of 'whether' this will happen; it is a question of 'when.'"

This time all the dots have been connected. This time the warnings are loud and clear, and we must heed them.

In contrast to the known threat of cyber attacks, another persistent challenge we face comes from those threats we fail to even anticipate—the so-called “black swan” events that test our assumptions. These are our most vexing problem because we cannot simply build walls around every potential target. Nonetheless, if we strengthen information sharing and analytic capabilities, our law enforcement and intelligence officers can disrupt more plots, whether they are those we know well or ones we have never before seen.

In my judgment, which is informed by numerous discussions with experts, the attack in Benghazi was not a “black swan” event but rather an attack that should have been anticipated based on previous attacks against Western targets, the plentiful, dangerous weapons in Libya, the presence of al-Qaeda, and the overall threat environment.

Whatever the plots hatched by our enemies, I am also concerned about vulnerabilities that stem from our own the government’s actions or failure to act.

I’ve already noted the lack of security in Benghazi, the grave, self-inflicted wounds from intelligence leaks, and the failure to enact a cybersecurity bill. There is also the genuine danger posed by the automatic, mindless cuts known as sequestration. Absent a commitment by the President and Congress to avoid this disastrous policy, the budget of every federal agency represented here today – agencies charged with protecting our nation from terrorism and other disasters – will be slashed in an indiscriminate way, by eight percent or more, potentially affecting vital programs such as border security, intelligence analysis, and the FBI’s work.

At a time when budget constraints require everyone to sacrifice, we should ask where resources can be spent more effectively and what tradeoffs should be made—to balance the risk we face with the security we can afford. What we cannot afford, however, is to weaken a homeland security structure that is helping to protect our country.