Statement of Ranking Member
Susan M. Collins

"Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration"

March 10, 2011

★ ★ ★

Effective information sharing among federal law enforcement and civilian and military intelligence agencies is critical. The 9/11 Commission found that the failure to share information across the government crippled efforts to detect and prevent the attacks on September 11th, 2001. Improving this communication was a critical part of the Intelligence Reform and Terrorism Prevention Act that Senator Lieberman and I authored in 2004.

The WikiLeaks breach should not prompt a knee-jerk retreat on the sharing of information and its use by those analysts who need it to do their jobs. We must not let the astonishing lack of management and technical controls that allowed a Private in the Army allegedly to steal some 260,000 classified State Department cables and 90,000 intelligence reports to send us back to the days before September 11th.

Unfortunately, we continue to see agency cultures that resist sharing information and coordination with their law enforcement and intelligence counterparts. Almost 10 years after 9/11, we still witness mistakes and intelligence oversights reminiscent of criticisms predating our reforms of the intelligence community. Among those cases where dots were not connected and information was not shared are: Umar Farouk Abdulmutallab, the so-called Christmas Day bomber, and Nidal Hasan, the Fort Hood shooter.

At the same time, there have been several cases that underscorce the incredible value of information sharing. An example is the case of Najibullah Zazi, whose plans to bomb the New York City subway system were thwarted.

As such successes remind us, we must not allow the WikiLeaks damage to be magnified twofold. Already, the content of the cables may have compromised our national security. There have been news reports describing the disclosure of these communications as having a chilling effect on our relationships with friends and allies. More important, they likely have put the lives of some of our citizens, soldiers, and partners at risk.

Longer lasting damage could occur if we allow a culture to re-emerge in which each intelligence entity views itself as a separate enterprise within

the U.S. counterterrorism structure, with each attempting to protect what it considers its own intellectual property by not sharing with other counterterrorism agencies.

Such a step backward would run counter to the policy goals embodied in the Intelligence Reform Act, articulated by law enforcement and intelligence community leadership, and underscored in multiple hearings before this Committee; that is, to effectively detect and interdict terrorists, the "need to share" must replace the "need to know."

I also would like to hear about the possible technological solutions to this problem. For example, my credit card company can detect out-of-the-ordinary charges on my account almost instantaneously. Yet, the military and intelligence community were apparently unable to detect more than a quarter million document downloads in less than nine months. Surely, the government can make better use of the technology currently employed by the financial services industry.

It is also notable that the intelligence community was already required to install some audit capabilities in its systems by the 2007 homeland security law, which could have included alerts to supervisors of suspicious download activity. Had this kind of security measure been in place, security officers might have detected these massive downloads before they were passed on to Wikileaks.

Technology and innovation ultimately should help protect information from unauthorized disclosure, while facilitating appropriate sharing of vital information.

I also would like to explore the implementation of "role-based" access to secure classified information. Instead of making all information available to everyone who has access to classified systems, under this model information is made available in a targeted manner based on individuals' positions and the topics for which they are responsible. Access to information not directly relevant to an individual's position or responsibilities would require a supervisor's approval.

We must craft security solutions for the 21st Century and beyond. We are in a world of Tweets and instantly viral videos on YouTube. We must strike the proper balance that protects classified and sensitive information with ensuring the sharing of vital data. We can use the most cutting-edge technology to protect the traditional tools of statecraft and intelligence – relationships and information.

###