Statement of Ranking Member
Susan M. Collins

"Ten Years After 9/11: A Status Report on Information Sharing."

October 12, 2011

★ ★ ★

The results of information sharing and collaboration within the Intelligence Community were evident in the operations that located, tracked, and killed Osama bin Laden and Anwar al Awlaki and just yesterday, in the disruption of a plot by elements of Iran's government to kill the Saudi ambassador to the U.S. on American soil. This appears to be another victory for the cooperation across departmental boundaries.

When the Chairman and I were working on the Intelligence Reform Law in 2004, we understood it would be challenging to change the culture in the intelligence and law enforcement communities from "need to know" to "need to share."

It is gratifying that many intelligence and law enforcement professionals have embraced this change. In a recent op-ed, Director of National Intelligence James Clapper observed that the Intelligence Community now starts "from the imperative of 'responsibility to share,' in order to collaborate with and better support" its intelligence consumers, "from the White House to the foxhole."

United States Attorney Patrick Fitzgerald more colorfully told an audience last month that intelligence and law enforcement operators now ask themselves: "[I]f it's found out that I have information that I didn't share with someone, how am I going to justify to myself that I sat on it?" He could have added: How will the failure to share be justified to Congressional overseers or, far worse, to the victims of a successful attack?

I believe the influx of new analysts who joined the Intelligence Community after 9/11 has had a real impact on information sharing. This new generation of intelligence officers is much more comfortable sharing information; social media and collaborative information technology have been a daily part of their lives. It just makes since that they would incorporate those same tools into their work.

Notwithstanding recent successes, however, the GAO continues to rank terrorism-related information sharing as a high-risk area. And, as we saw in the Fort Hood attacks and the attempted airplane bombing on Christmas Day 2009, when information is not shared, our nation's security is placed at risk.

The Bowling Green, Kentucky, case is another recent example of information apparently not being shared, and it remains very troubling to many of us.

It is unsettling that a suspected bomb maker, whose fingerprints we had had for years, was able to enter our country on humanitarian grounds.

I have raised this issue repeatedly with the Secretary of Homeland Security and the FBI Director. Both have told this committee the 58,000 individuals who have been settled in the U.S. have been vetted against the existing databases. But it is clear that those databases are still incomplete. Forensic information being collected from IEDs in war zones should be shared and used to screen those seeking to enter our country.

In some respects, these cases may demonstrate an evolution of information sharing: As more and more information is being shared, it is increasingly important for agencies to think creatively about how best to prioritize, analyze, and act upon that information. As this Committee concluded in our investigation of the Fort Hood shootings, the Defense Department and the FBI collectively had sufficient information to have detected Major Hasan's radicalization to violent Islamist extremism, but they failed to act effectively on the many red flags signaling that he had become a potential threat.

As Wikileaks breach demonstrates, we also need to secure data from internal threats. We must be vigilant, however, to ensure that such security measures do not recreate old stove-pipes. Technology and innovation should ultimately help protect data from unauthorized disclosure, while facilitating appropriate sharing of vital information.

Just last week, the President signed a new Executive Order on "Responsible Information Sharing" prompted, in part, by the Wikileaks situation. This hearing should help us assess the President's new order.

The President's new Executive Order will create a "Classified Information Sharing and Safeguarding Office" within the Information Sharing Environment we established in the 2004 law. Unfortunately, according to GAO, this framework is still not as strong as it could be.

As we explore the issue of information sharing, we must also ensure that our homeland security partners, like local law enforcement and fusion centers, are receiving and sharing information that is useful and adds value. Among other things, the Intelligence Community must clearly identify what sorts of data are needed, so state and local partners can be on the lookout for the most useful bits of information.

The public should be able to share its information too. This is why Senator Lieberman and I introduced our "See Something, Say Something" bill, so the public can more easily share – and law enforcement professionals can act on – their tips.

Finally- I would be remiss if I did not express my concern over this administrations inexplicable failure to fully appoint and staff the privacy oversight board that we created as part of our 2004 act. I am truly baffled by the administrations slowness in this regard because it is an important check as we seek to expand information sharing. From the most sophisticated intelligence collection methods to the police officer on the street to the observant sidewalk vendor, information sharing is key to keeping our fellow citizens safe.