Committee on
HOMELAND SECURITY
Chairman Peter T. King

Opening Statement

April 26, 2012

Media Contact: Shane Wolfe

(202) 226-8417

Statement of Chairman Meehan

Subcommittee on Counterterrorism and Intelligence and Joint Hearing

"Iranian Cyber Threat to the U.S. Homeland"

April 26, 2012
Remarks as Prepared

I would like to begin today by thanking Chairman Lungren and Ranking Member Clarke, and all the members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies for joining us here today to examine the threat posed by Iran in the cyber arena. The combination of our expertise on counterterrorism and intelligence and your expertise on cyber security will inform and enhance our discussion, and I look forward to hearing from you and our panel.

I believe this joint hearing represents the attitude we must have when confronted with emerging threats that may not be adequately understood. In my view, the adaptability, flexibility, and willingness to erase institutional barriers called for in the 9/11 Commission Report is on display here, with each of us bringing our own expertise to study a threat which crosses borders and cannot easily be put into one box. While Chairman Lungren and his colleagues on the CIPST Subcommittee have studied the 'ins' and 'outs' of protecting our nation's critical infrastructure from cyber attack, the members of the CTI Subcommittee have spent a lot of time examining the threat posed by Iran, the world's largest state sponsor of terrorism, and its proxies, including Hezbollah.

For the Subcommittee on Counterterrorism and Intelligence, this hearing is a continuation of our previous work examining the threat from Tehran. Last year, our subcommittee examined the Hezbollah presence in Latin America that detailed the recently exposed Iranian government plot to conduct a brazen terror attack here in Washington, D.C. I have also recently returned from the region, where I met with defense and intelligence officials and government leaders in Israel, Turkey, and Jordan. After in-depth conversations and briefings, including with Turkey President Abdullah Gul, Israeli Prime Minister Benjamin Netanyahu, and His Majesty King Abdullah of Jordan, it became increasingly clear that Iran is the most destructive and malicious actor in the region and will persist in antagonizing the United States and our allies, especially the State of Israel.

As Iran's illicit nuclear program continues to inflame tensions between Tehran and the West, I am struck by the emergence of another possible avenue of attack emanating from Iran: the possibility that Iran could conduct a cyber attack against the U.S. Homeland.

Many will discount this threat – just as many ignored the possibility that Iran would conduct an attack on American soil. This assumption was proven woefully wrong when last year's plot to kill the Saudi Ambassador was uncovered. Now that we are adjusting to a realistic understanding of Iran's intent to conduct terror attacks and kill innocent Americans in the U.S. Homeland, we cannot blind ourselves to this new threat. After all, if Iran is willing to blow up a Washington restaurant and kill innocent Americans, we would be naïve to think Iran would never conduct a cyber attack against the U.S. Homeland.

Earlier this year in testimony before the Senate Intelligence Committee, Director of National Intelligence James Clapper clearly stated: "Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity." In what I view as a private sector validation of the cyber threat posed by Iran, Google Executive Chairman Eric Schmidt recently stated, the "Iranians are unusually talented in cyber war for some reason we don't fully understand." And, in the event of a military strike against Iranian nuclear facilities, former Director of the National Counterterrorism Center Michael Leiter assessed that a cyber attack conducted by Tehran against the US would be "reasonably likely."

The threat of cyber warfare may be relatively new – but it is not small. Iran has reportedly invested over $1 billion in developing their cyber capabilities, and it appears they may have already carried out attacks against news organizations like the BBC and Voice of America. There have been reports that Iran may have even attempted to breach the private networks of a

major Israeli financial institution. Iran is very publicly testing its cyber capabilities in the region and, in time, will expand its reach.

Other nations such as Russia and China may have more sophisticated cyber capabilities, but there should be little doubt that a country that kills innocent civilians around the world, guns down its own people, and calls for the destruction of the State of Israel would not hesitate to conduct a cyber attack against the U.S. Homeland. That is why today's hearing is so important.

I want to thank all of you for joining us today, and I look forward to hearing from our witnesses.

###