Opening Statement - Ranking Member Cedric L. Richmond

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"The Role of Cyber Insurance in Risk Management"

March 22, 2016

Unfortunately, businesses and government in America, and across the world, are seeing increased levels and frequencies of cyber attacks and the rapidly accelerating sophistication of state-sponsored and privately organized cyber criminals. Over the past few years, this Subcommittee has conducted government oversight and produced legislative initiatives and worked diligently to provide the Department of Homeland Security and other federal agencies, with the tools it needs to protect our systems and databases, and encourage the participation of private industry both in the critical infrastructure sector and for information sharing.

Today, we are going to hear from private industry, and a representative of their state insurance regulatory Commissioners about Cyberinsurance. While, the Full Committee, and particularly this Subcommittee, has no oversight or legislative jurisdiction over the Cyberinsurance activities of these actors and sectors, we do have an interest in how they are doing.

The statistics are familiar to us all, the percentage of U.S. critical infrastructure assets owned by private sector firms is estimated to be somewhere in the neighborhood of 85 percent. The way these assets are operated and managed has vastly changed over the last few decades due to the impact of the digital revolution related to computer-based information systems. These changes have increased the efficiency associated with using our infrastructure assets.

The digital revolution, however, has also created serious risks to the nation's critical infrastructure due to actual and potential cybersecurity breaches. As noted by President Obama in his Executive Order on Cybersecurity, February 12, 2013: *Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.*

Last year set a high bar for the size and scope of data breaches, led by the theft of over 20 million government background checks, and with that high bar, an increasing interest in how state and local governments, and businesses large and small, can manage their risks and vulnerabilities when they operate in cyberspace.

For example, recently on a panel on '*lessons learned'* from real-world Chief Information Security Officers', the University of Virginia's Randy Marchany explained that the increased and sophistication of the level of today's cyber threats forces him to assume that hackers already have access to his network, and the best he can do is to monitor for when the latent threat becomes active.

With that said, let's cut to the chase—what would a Cyberinsurance policy look like if an experienced Chief Information Security Officer, or CISO, of a company or municipal government came to your insurance company with the proposition that it is likely that his systems had already been hacked and the malware was likely dormant, but he wanted to purchase insurance from you as to mitigation and repercussions?

Or, to complicate things even more, and introduce the well-known 'moral hazard' consideration that accompanies any insurance policy—what if a hypothetical CISO knew he had been hacked, but wasn't telling you or anyone else, and he knew or suspected the hack or intrusion was lying dormant and would activate at some later date? I am not the first to pose these kinds of questions, and these are questions I am sure all of us have had, if you contemplate the issue of Cyberinsurance at all.

But these are worst-case scenarios. Going forward, Cyberinsurance can play a key role in helping businesses, especially small and mid-sized business, to assess their cybersecurity posture and readiness, and their ability to be resilient and recover from anticipated cyber threats and attacks. We are engaged in an exceptionally complex and nuanced policy arena. I am especially interested to see how the states will handle the regulatory responsibilities that surround Cyberinsurance, and how the states can serve as incubators for innovative solutions to the national, international, and industry-wide challenge of cybersecurity for our nation's businesses and government agencies.