Opening Statement of Chairman Devin Nunes,

House Permanent Select Committee on Intelligence

Hearing on Worldwide Cyber Threats

September 10, 2015

Thank you, Director Clapper, for assembling the panel of witnesses for this morning's hearing on Worldwide Cyber Threats. We know your time is extremely valuable and appreciate you updating this committee and the public on the threats we face around the world.

This committee has traditionally hosted an open worldwide threats hearing to better educate the public on the current dangers we face, as well as showcase how the intelligence community is working to combat these threats. The focus of this hearing is cyber security—or given the current state of affairs, cyber *insecurity*.

Over the last several years, cyber-attacks have become commonplace in the United States. Anthem, Home Depot, Sony, Target, JP Morgan Chase, and other companies have been subject to major attacks, resulting in the compromise of personal information of employees and customers alike. But these are just the breaches we hear about in the news. There are many more, both large and small, occurring each and every day across our nation.

The U.S. government is certainly not immune. OPM, IRS, the Pentagon's Joint Staff, and just this morning we learned that the Department of Energy was successfully hacked 159 times. These high-profile assaults are eroding confidence in our government's ability to counter the threat. I share the public's concern. In fact, I recently learned that the very apparatus that the Department of Homeland Security uses to allow the private sector to share cyber-threat indicators with the government—the Protected Critical Infrastructure Information Program—has not had a security audit since 2006. This raises serious questions about an Agency that many government representatives believe should be at the heart of our cybersecurity strategy.

I want to place the intelligence community on notice that we will be requesting information regarding your cybersecurity practices and procedures in the coming months. The government should not even think to impose standards on the private sector before it can maintain the security of its own systems.

As Congress continues to debate information-sharing legislation, we must ensure that government entities involved in the sharing process are absolutely secure—especially if we allow the private sector to share cyber-threats with just one government entity, such as DHS.

In closing, I call on the Senate to take up cyber-sharing legislation. Seemingly every day, another breach is exposed with severe implications for our economy, our privacy, and our national security. The time has come to put politics aside and give our country the tools it needs to defend itself from these malicious attacks.