HOMELAND SECURITY
COMMITTEE

Statement of Chairman Michael McCaul (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee

"Oversight of the Cybersecurity Act of 2015"
June 15, 2016

Remarks as Prepared

Before I start today, I would like to say a few words about the tragic events in Orlando. Our thoughts and prayers go out to the victims and their families, and our deepest gratitude goes out to the first responders who helped save lives.

It was the deadliest terrorist attack on the U.S. homeland since 9/11, but our response has shown that Americans are resilient and will not be intimidated by extremists.

Yesterday I moderated a classified briefing on the investigation with the heads of DHS, the FBI, and the National Counterterrorism Center, and in the coming months we will continue to seek answers. We will also take action to protect our country and prevent such an attack from happening again.

The events in Orlando are a reminder that our nation is being targeted by those who want to undermine our freedom and diminish our prosperity.

But the threat is not just from terrorists. Today we will discuss how our nation is also being targeted and attacked—in real-time—by faceless intruders across the web.

As we speak, a war is being waged against us in cyberspace. Criminals, hacktivists, violent extremists, and nation-states are infiltrating our networks and infecting our systems. Their motives are to deceive, steal, and destroy, and the impacts of their attacks are felt everywhere— from our kitchen tables to corporate boardrooms.

This Committee has made our nation's cybersecurity a top priority, and in recent years we have passed a number of landmark cybersecurity bills.

First, we established a federal civilian interface at the National Cybersecurity and Communications Integration Center, or NCCIC, to facilitate cyber-threat information sharing.

This allows the government to communicate more effectively across 16 critical infrastructure sectors and with the private sector.

Second, we laid down the rules of the road regarding how information is shared—making sure data exchanges are efficient, timely, and secure.

Third, we put in place measures to keep Americans' rights and personal information protected.

Fourth, we made sure DHS was able to hire and retain top cybersecurity talent, because we cannot protect our networks without a cyber workforce that is smart and aggressive.

And fifth, we enhanced the Department's ability to prevent, respond to, and recover from cyber incidents on federal networks.

Those measures went a long way in helping us secure our systems. But even with the fundamentals in place, we still saw major vulnerabilities, especially the lack of information sharing.

After 9/11, we learned that if our agencies did not connect the dots, we could not stop attacks.

The same principle applies to cyber threats. If no one shares data, everyone is less secure and intrusions go undetected.

We realized that companies were very hesitant to share their sensitive data, so last year we drafted and passed the Cybersecurity Act to get the information flowing.

The law now provides liability protections so that companies and other organizations can more freely exchange threat indicators.
This includes "government-to-private" information sharing and "private-to-private" sharing.

The legislation was a major win for security and privacy, allowing companies to secure their networks and keep hackers away from our bank accounts, health records, and other sensitive information.

But we cannot be satisfied with this progress. We've got to be as aggressive as our adversaries—and we should aim to stay a step ahead of them.

I hope today our witnesses will help us understand how we can do exactly that—and how we can effectively implement this law to enhance America's digital defenses.

Thank you.

###