



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

*Opening Statement*

April 14, 2015

**Media Contact:** Susan Phalen, April Ward  
(202) 226-8477

---

**Statement of Chairman Michael McCaul (R-Texas)  
Committee on Homeland Security**

**Markup of H.R. 1731, the “National Cybersecurity Protection Advancement Act”**

**Remarks as Delivered**

We are here today to markup a cybersecurity bill that will increase awareness of cyber threats and help American companies and the United States government better protect their cyber networks. I want to commend our minority counterparts, both Ranking Member Thompson and Subcommittee Ranking Member Richmond for their collaboration and input on this important cybersecurity legislation. I truly hope and expect that we can pass this bill here today. And I’d also like to thank Chairman Devin Nunes’ House Intelligence Committee and Adam Shift, the ranking member, for their coordination and input as we all work together to address this issue that is vital to defending our homeland.

American computer networks are under siege. Government systems, private company networks, and private citizens’ computers, no one is immune. Every minute of every day, cyber attacks happen across the country—our government networks are being hacked, the intellectual property of U.S. companies is being stolen, and Americans’ personal information is being compromised. And in many cases, these attackers are not held responsible.

The recent breach at Anthem illustrates how easy it is for ordinary Americans to become victims of cyber attacks. This attack followed significant intrusions at Target, Neiman Marcus, Home Depot, and JP Morgan—all of which were designed to steal the personal information of private citizens.

As we have seen with the hacks on the State Department and the White House recently, nation-state actors like Russia, China, and Iran are increasingly breaching government networks and U.S. companies to conduct espionage or steal intellectual property.

In one of the most destructive cyber attacks last year, North Korea used a digital bomb to destroy computer systems at Sony Pictures in an apparent attempt to terrorize Americans and suppress freedom of speech and expression.

Make no mistake: such attacks are costing Americans their time, their money, and their jobs.

But the most malicious threat is a major cyber attack that shuts down the power grid, cuts off the water supply, or disrupts our gas pipelines. This could bring the critical infrastructure we use every day to a halt, cripple our economy, and weaken our ability to defend the United States.

These scenarios sometimes sound alarmist, but we must take them seriously because they grow more realistic every day.

To defend America's vital digital networks the public and private sector must work together.

The Department of Homeland Security's (DHS) center for integrating cyber threat information is the National Cybersecurity and Communications Integration Center (NCCIC).

The NCCIC is not a cyber regulator, it cannot prosecute you, and it is not a military or a spy agency. It's a civilian interface to the private sector.

Unfortunately, in the current environment, companies do not feel they have the adequate legal protection to share vital cyber threat information with the federal government.

Industry needs a "safe harbor" where legal barriers are removed, appropriate privacy protections are in place, and companies are incentivized to be a full participant with the NCCIC.

This bill, the National Cybersecurity Protection Advancement Act, creates this "safe harbor" by providing liability protections for the voluntary sharing of cyber threat information with the NCCIC or between private entities.

The bill also protects the privacy and civil liberties of all Americans by ensuring safeguards are in place to remove personal information before cyber threat information are shared.

We cannot tolerate acts of cyber vandalism, cyber theft, cyber terrorism, and cyber warfare especially when they put our nation's critical infrastructure and secrets at risk.

This bill will increase what we know about digital threats and, in doing so, will enhance American security while protecting Americans' privacy. Now is the moment to act.

###