



Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

March 13, 2013

Media Contacts: Mike Rosen, Charlotte Sellmyer
(202) 226-8417

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

**“DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical
Infrastructure”**

**March 13, 2013
Remarks as Prepared**

I would like to thank all of our witnesses for testifying today. Deputy Secretary Lute is testifying for the Department but I look forward to seeing Secretary Napolitano in the coming weeks to discuss DHS’ budget and its plan to maintain operations during these challenging times.

The chart on the screen depicts the roles of each major agency protecting our nation from cyber attacks.

The significance of this agreed-upon relationship to our national security is paramount. Each and every agency depicted understands their roles and responsibilities, working in tandem to keep America safe.

The purpose of this hearing is to examine the Department of Homeland Security’s (DHS) role, capabilities and challenges concerning cybersecurity. There are many issues facing the Department.

Today’s hearing is an opportunity to focus on the cyber threats facing our homeland and how together, we can defend against them.

Cyber attacks come in all forms. America is the victim of cyber espionage. Countries steal our military and intelligence information. There are threats of cyber-warfare from terrorists, and economic cyber attacks from Iran and China. These countries are stealing our trade secrets and intellectual property. The most daunting is undoubtedly the cyber threats against our critical infrastructure.

We know that foreign nations are conducting reconnaissance on our utilities – they are penetrating our gas and water systems and also our energy grids – and if the ability to send a silent attack through our digital networks falls into our enemies’ hands, this country could be the victim of a devastating attack.

Yet while threats are imminent, no major cybersecurity legislation has been enacted since 2002.

Imagine months without power. An attack on our transformers could cripple our power grids and our economy would follow. This is not science fiction; it is reality. A report recently released by Mandiant confirmed China is the source of nearly 90% of cyber attacks against the United States. Most troubling is that these hackers targeted a company that provides remote access to more than 60% of North America’s oil and gas pipelines.

Hackers have also attacked the servers of our Air Traffic Control System, and just last year, an al Qaeda operative issued a call for “electronic jihad” against the United States – comparing our technological vulnerabilities to that of our security before 9/11.

Iran and Russia are some of the world’s worst offenders. Last December, Iranians attacked the state-owned Saudi Aramco, with the goal of stopping Saudi Arabia’s oil production. Additionally, this year Iran conducted multiple denial of service attacks on major U.S. banks.

Unlike 9/11, we have seen the warning signs—now it is time to act. For us to defend against cyber attacks we must designate roles for all of the key agencies—DHS, DoD and the Justice Department. Each play a crucial role defending our homeland against cyber threats and none can do it alone.

When DHS was established, the Secretary of DHS was made responsible for “coordinating the overall national effort to enhance the protection of our critical infrastructure.”

The National Infrastructure Protection Plan (NIPP) and the recent Executive Order solidified DHS’ role as the lead federal agency in protecting domestic critical infrastructure.

Most importantly, the agencies themselves agree that a framework where DOJ is the lead for investigation, DHS is the lead for protection and DoD as the lead for defense would allow each

department to concentrate on their core mission with, as General Alexander once said, "...DHS as the entry point for working with industry."

In order to fulfill this role as a civilian command center, DHS has been building its partnerships with the private sector and growing its capacity as an effective conduit for threat information sharing. DHS manages a bottom-up network of entities from local first responders to nationwide threat analysis and emergency response centers like the National Cybersecurity and Communications Integration Center (NCCIC).

The Department possesses the ability to provide real time information necessary for instant threat detection, and to share emerging threat information to enable industry to act immediately to safeguard critical infrastructure. Additionally, DHS has a well-developed Privacy Office to protect Americans' privacy and civil liberties.

While the Department has made great progress, there are areas for further improvement across the board when dealing with cyber threats. Legal barriers, regulatory uncertainty and a lack of resources remain challenges. Additionally, there is not enough private sector participation in the programs that are already in place, because they either don't have the resources or don't see the value in doing so.

Congress has the ability and the obligation to help fix these problems. For us to thwart attacks, we must build upon the executive branch's efforts and work with all stakeholders to find the consensus necessary to protect this country. As part of this commitment, the Continuing Resolution recently passed by the House includes an increase of \$282 million for cybersecurity over fiscal year 2012 levels.

Hearings like the one today will help guide the legislative process. I look forward to listening to all of our witnesses about what works, what doesn't and what we can do to streamline our cyber defenses.

One of the primary lessons from 9/11 is that only by working together can we detect and deter our enemies. In the wake of that tragedy, the walls preventing agencies from sharing threat information became apparent. We cannot allow turf battles to hinder us from developing the defenses necessary to prevent cyber attacks. The threat is real, and this time we see it coming.

###