

Statement of Senator Orrin G. Hatch
On the Floor of the U.S. Senate
Regarding Introduction of
National Cyber Infrastructure Protection Act
June 24, 2010

Senator Hatch – Mr. President, today I rise to express my support as a cosponsor of the National Cyber Infrastructure Protection Act. At long last, our nation is finally recognizing the increasing danger posed by cyber threats and the devastating disruption that they can cause because of the interdependent nature of information systems that support our nation's critical infrastructure.

As a nation, we must develop a strategy that provides a strategic framework to prevent cyber attacks against America's critical infrastructures. As a government, we must reduce national vulnerability to cyber attacks and minimize the damage and recovery time from cyber attacks should they occur. I believe that the legislation that my colleague from Missouri and I are introducing today will provide a sure foundation to put our nation on a path to begin to address cyber vulnerabilities.

The challenge to protect cyberspace is vast and complex and ultimately requires the efforts of the entire government. As a nation, we must recognize that cyber threats are multi-faceted and global in nature. These threats operate in an environment that rapidly changes. The sharing of information between government and the private sector is crucial to our overall national and economic viability.

Last January, McAfee issued a report that concluded that the use of cyber attacks as a strategic weapon by governments and political organizations is on the rise. The U.S. is the most targeted nation in the world -- and our military, government and private sector systems are often attacked with impunity. Our nation has experienced large-scale malicious cyber intrusions from individuals, groups and nations. These attacks have dramatically increased in number and complexity.

Just last year, Google and over 30 other companies linked to our energy, finance, defense, technology and media sectors fell prey to costly cyber attacks. Too many nations either directly sanction this activity or give it tacit approval by failing to investigate or prosecute the perpetrators. Many of the major incidents are presently coming out of Russia and China.

The National Cyber Infrastructure Protection Act would establish a National Cyber Center, housed within the Department of Defense. The mission of the National Cyber Center would be to serve as the primary organization for coordinating federal government defensive operations, cyber intelligence collection and analysis, and activities to protect and defend federal government information networks. Critical in achieving this mission would be the sharing of information between the private sector and federal agencies regarding

cyber threats. This center would be led by a Senate-confirmed Director modeled after the Director of National Intelligence position. The Director reports directly to the President and would coordinate cyber activities to protect and defend federal government information networks. The Director would serve as the President's principal adviser on such matters and developing policies for securing federal government information networks.

In our nation today, over three-fourths of our nation's critical infrastructure is under the control of the private sector. One such example is smart grid technology for power grids. The Smart Grid will use automated meters, two-way communications and advanced sensors to improve electricity efficiency and reliability. The nation's utilities have embraced the concept and are installing millions of automated meters on homes across the country. However, cyber security experts have determined that some types of meters can be hacked. As we rely on technology developed by private industry, we must ensure that we harden this technology against threats that could leave our citizens vulnerable.

The opening salvos of future conflicts will be launched in cyberspace. In 2008, we saw this occur when Russian forces launched a cyber attack on Georgian defense and information networks. The Russians essentially blinded the Georgian military during the South Ostessia conflict. Our reliance on technology and integrated networks certainly makes our military and critical infrastructure more efficient. However, that efficiency can have its price in the form of cyber vulnerability.

As Americans, we must be prepared to fight back should we be attacked. We must also harden our networks against the tools that criminals use to steal a person's identity and a company's trade secrets. These are the same tools that today can and will be used by terrorists in the future to attack and erode our infrastructure and defense systems. The stakes are too high and the risks are too grave to delay. If we don't move now to protect our national cyber infrastructure, the consequences to our economy, security and citizens could be dire. This is a fight we must win. The only way to win is to be prepared.

Mr. President, I yield the floor.