Statement of Ranking Member
Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"

November 17, 2010

★ ★ ★

Today's hearing focuses on cyber threats to our nation's most critical infrastructure.

Much attention has been paid to cyber crimes such as identity theft and to cyber attacks intended to steal proprietary information or government secrets. But lurking beyond those serious threats are potentially devastating attacks that could disrupt, damage, or even destroy some of our nation's critical infrastructure, such as the electric power grid, oil and gas pipelines, dams, or communication networks. These cyber threats could cause catastrophic damage in the physical world.

This threat is not theoretical. It is real and present. The newest weapon in the cyber toolkit was introduced to the world in June, when cybersecurity experts detected a cyber worm called Stuxnet.

It was clear to cybersecurity experts that Stuxnet was extraordinarily sophisticated malware, whose complexity was something no lone hacker could achieve. With more than 4,000 functions, the worm's complex code was longer than much of the commercial software we use on our computers every day. The development of this sophisticated attack was likely the work of a well-financed team of experts with intimate knowledge of the targeted systems.

Stuxnet was programmed specifically to infiltrate certain Industrial Control Systems (ICS), allowing the worm potentially to overwrite commands and to sabotage the infected systems. It was discovered in July at the Bushehr power plant, Iran's controversial nuclear power facility. It was also found in systems in China, Indonesia, India, the United States, and elsewhere. More than 100,000 computers have been infected.

Industrial control systems, like the Siemens systems affected by Stuxnet, are widely used in electric power plants, water and wastewater treatment, the oil and natural gas industry, transportation, and manufacturing. Malware like Stuxnet has the potential to change instructions, commands, or alarm thresholds, which, in turn, could damage, disable, or disrupt equipment.

After four months of reverse-engineering Stuxnet, cyber experts at the Department of Homeland Security, Symantec, and other researchers concluded

that this malware was capable of incredibly dangerous impacts. The *Christian Science Monitor* noted that cybersecurity experts identified Stuxnet as the world's "first known cyber super weapon designed specifically to destroy a real-world target –- a factory, a refinery, or just maybe a nuclear power plant."

If a cyber attack like this worm were launched on a large transformer on the electric power grid, for example, the impact could cascade, potentially leaving large regions of the United States without electricity, halting our economy, and undermining our national security. The cyber threat is urgent, and the consequences of a major national cyber attack could be devastating.

To develop a comprehensive approach to this national threat, Senator Lieberman, Senator Carper, and I have introduced bipartisan legislation to strengthen our cyber defenses across both the federal government and the private sector.

Unanimously approved by this Committee in June, our bill would fundamentally reshape how the federal government works collaboratively with the private sector to address all cyber threats, from espionage and cyber crime to attacks on the most critical infrastructure.

For our nation's most critical systems and assets, whose disruption would cost thousands of lives or multiple billions of dollars, the bill would establish certain risk-based performance requirements to close security gaps.

These requirements would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted. The owners and operators of these systems would be able to choose which security measures to implement to meet applicable risk-based performance requirements. This model would allow for continued innovation that is fundamental to the success of the IT sector.

The President's authority to deal with a catastrophic cyber attack aimed at critical infrastructure would be carefully defined -- and constrained. The President would not have the authority to take over critical infrastructure.

The Stuxnet worm demonstrates that cyber attacks reach beyond threats to identity, intellectual property, and the economy, and can produce serious, potentially devastating effects on critical infrastructure.

The Department of Homeland Security's Control Systems Security Program (CSSP) has made much progress in supporting owners and operators of critical infrastructure to address cyber vulnerabilities to industrial control systems. We must build on these partnerships.

Despite the progress made by DHS, the government's overall approach to cybersecurity remains disjointed and uncoordinated. The threat is too great to allow this to continue. The need for Congress to pass comprehensive cybersecurity legislation is more urgent than ever.

# # #