S. 3480, THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT

The first item on our agenda today is S. 3480, whose purpose is to Protect Cyberspace as a National Asset, which I was pleased to introduce along with Senators Collins and Carper. This is important legislation that is urgently needed to modernize, strengthen, and coordinate our cyber defenses, while increasing the preparedness and resiliency of the critical infrastructure upon which we so utterly depend.

Given our nation's reliance on the Internet to run our most critical infrastructure, the potential damage from a concerted cyber attack is equal to, if not greater than, what we might experience from a conventional military attack on our homeland. A full-scale cyber attack could turn off our electricity and all that we run on it; it could cause generators to burn out, pipelines to explode, and dams to fail and could lead to the death and injury of thousands of people, and could cost our economy billions of dollars. This is no longer fantasy or fiction. It is a clear and present danger.

Our Committee has found that America's current cyber defenses are disjointed, understaffed, and under-resourced. We need leadership to remedy these shortcomings, an organizational structure that requires everyone to play by the same rules, and incentives for the private sector to join in this effort to secure the critical infrastructure that it owns.

Our bill, S.3480, would fundamentally reshape the way the federal government defends America's cyberspace. Our bill would create a White House Office of Cyberspace Policy, led by a Senate-confirmed director, to coordinate federal government and private industry efforts to defend America's cyberspace.

Our dot.gov networks and assets need better protection, as do the privately-owned networks that run our most critical infrastructure. The DHS Inspector General recently issued a report highlighting how DHS's current cyber security operations are impaired by a lack of clear lines of authority. Our bill would address this by creating a National Center for Cybersecurity and Communications – to be located within DHS – with

authority to implement security measures for civilian-government networks and for those critical networks owned by the private sector.

The defense of our cyber networks cannot succeed without the cooperation of the private sector. That's why our bill would establish a private-public sector partnership enabling both sectors to work together to meet a baseline set of security requirements that DHS would enforce.

Thanks to Senator Carper's efforts, our legislation also reforms and updates the Federal Information Security Management Act (FISMA) to require continuous monitoring and protection of federal networks while doing away with the time-consuming paper-based reporting system.

In the event of a catastrophic cyber attack that could seriously jeopardize public safety, our economy, or our national security, the bill provides the President with the authority to initiate emergency measures to protect our most critical infrastructure.

You may be aware of alarmist traffic in the blogosphere claiming our legislation would give the President a "kill-switch" for the internet. What these reports fail to recognize is that, to the extent such a "kill

switch" is even technologically feasible, the President already has that authority. Under section 706 of the 1934 Communications Act, the President, if he wanted to, could arguably take over or shut down much of the nation's communications systems in the event of an actual or impending attack.

What is new and innovative about our bill is that we give the President a range of options to address the most severe threats. Our bill provides the President with a scalpel to address threats to individual systems or networks, so he can *avoid* using the sledgehammer of shutting down entire communications networks. Our bill requires that any emergency measure be the least disruptive step necessary to protect the system or network affected.

Cyber attacks pose a real and urgent threat, which we ignore at our peril. This legislation takes a comprehensive, risk-based, and business-oriented approach to addressing critical vulnerabilities in our own defenses. We believe our bill would go a long way toward improving

the security of our government and private critical infrastructure, and therefore the security of the American people.

Senator Collins, Senator Carper, and I have a substitute amendment – which incorporates suggestions we received from members of the Committee, witnesses at our hearing, privacy and civil liberties advocates, and representatives of the private sector – that I would like to introduce at this time.

The substitute would make a number of clarifying edits to the underlying bill including: more clearly defining the scope of the critical infrastructure covered by the mandatory requirements in Sections 248 and 249; establishing a redress process for owners of covered critical infrastructure who believe they were erroneously added to the list; and ensuring that members of the private sector are appropriately incorporated into federal cyber security efforts.

The substitute also requires DHS to complete an identity management plan for cyberspace, an issue that White House Cyber Security Coordinator Howard Schmidt highlighted as a priority in a

speech earlier this week. Lastly, the substitute requires Congressional approval should the President wish to extend the application of emergency measures beyond 120 days.

I want to thank Senators Pryor, Ensign, McCaskill, and Coburn for working with us on important provisions within the substitute amendment.