

Opening Statement of
Senator Susan M. Collins

'Cybersecurity: Developing a National Strategy'

Committee on Homeland Security and Governmental
Affairs

April 28, 2009



The information and communications networks we refer to as cyberspace have become critical to our economy, national defense, and homeland security. Yet every week, we learn of more threats to our cyber infrastructure. The specter of our adversaries disrupting our telecommunication system, shutting down our electrical power, or freezing our financial markets is not science fiction. It is a very real possibility as thousands of attacks occur every day. For example:

- **Intelligence officials have stated that China and Russia have attempted to map the United States' electrical grid and have left behind software that could be activated later, perhaps to disrupt or destroy components;**
- **The *Washington Post* has reported that hackers broke into the Pentagon's Joint Strike Fighter project and stole information; and**
- **Last year, cyber thieves secretly implanted circuitry into keypads sold to British supermarkets, which were then used to steal account information and PIN numbers.**

As these intrusions demonstrate, the cybersecurity threat is real, dangerous, and accelerating. Today this Committee will examine the practical issues of how we

should organize the federal government to respond effectively. An effective response to cyber threats will require coordination among law enforcement, intelligence agencies, and the private owners of critical infrastructure. The Department of Homeland Security is the crucial nexus of these realms.

Bringing together these three worlds is precisely the reason Congress created DHS following the terrorist attacks of 9/11. The Comprehensive National Cybersecurity Initiative, started last January, recognized the value of the Department's unique perspective by placing the National Cyber Security Center at DHS and charging DHS with responsibility for advancing coordination and consultation among the many federal entities with cybersecurity missions.

Last year, Senator Lieberman and I included cybersecurity provisions in the Homeland Security authorization bill that would have increased the responsibilities of the National Cyber Security Center in DHS.

We need to determine what authorities are necessary for DHS to undertake the mission of better securing federal networks and our nation's critical cyber infrastructure – authorities that must be exercised as the Department works with, but does not supplant, the important roles played by the Department of Defense, the Intelligence Community, federal law enforcement officials, and other agencies.

These authorities must allow the federal government to address some of the most pressing cybersecurity issues, including:

- **Sharing critical information on threats and vulnerabilities with the private sector since 85% of critical infrastructure is privately owned;**
- **Encouraging the adoption of best practices and standards across the government and throughout our nation's critical infrastructure;**
- **Generating a strategy that deters terrorists and hostile nation-states from executing cyber attacks that could potentially devastate our critical infrastructure;**
- **Securing the supply chain to ensure that the systems we purchase are free from malicious code; and**

- **Establishing standards and performance metrics that can guide government procurement and so encourage manufacturers to incorporate better security into their products for the benefit of both the government and the public at large.**

Finally, as we consider the organization of our cybersecurity activities, I would note this new Administration has shown a tendency to appoint special assistants and czars within the White House for virtually every problem that comes along. While I understand the need to shine a spotlight on these problems, the creation of numerous czars or special assistants usually leads to conflict, turf battles, and confusing lines of authority.

Moreover, Congress's ability to effectively oversee activities directed from the Executive Office of the President is severely limited. Typically, we cannot call

on those in the White House to testify before us, and their budget requests have limited detail. On an issue as pressing and complex as cybersecurity, congressional oversight is crucial to making real progress.

I hope to explore these issues with the witnesses today so that we can provide the basis for legislation to provide DHS with the authorities it needs to secure our nation's information technology systems. As the recent intrusions attest, this issue requires our attention.

#