

Cyber Security: Developing a National Strategy
Committee on Homeland Security and Governmental Affairs
Chairman Joe Lieberman
April 28, 2009

AS PREPARED FOR DELIVERY

Good morning and welcome to our hearing on developing a national strategy for cyber security. We've called today's hearing to ask some basic questions: how prepared is our government to prevent and respond to the very serious threat of cyber attacks against America and how can we help the Department of Homeland Security perform this critical mission?

After the September 11th terrorist attacks and the creation of the Department of Homeland Security, safeguarding our information networks became a top priority. Congress gave DHS responsibility to assess and track cyber vulnerabilities, but that responsibility has not been carried out as well as any of us had hoped.

The Obama Administration -- has now completed an urgent 60-day review of cyber policy and structures and we await public release of the review with the expectation it will greatly inform a national strategy

to ensure that all agencies and departments, in concert with our private sector partners, are working to raise our cyber guard.

I wish we were farther down the road toward clarity of purpose and unity of effort in this endeavor because it is clear our cyber infrastructure is now under constant attack. Our enemies – whether they are individual hackers, foreign governments, business competitors, organized criminal groups, or terrorists – are one step ahead of our efforts to deter them. That gap must be closed.

From 2003's SQL Slammer to the most recent Conficker worm, thousands of worms, viruses, and so-called "malware" have infected and disabled computers around the world and put sensitive data at risk of loss, theft, or improper disclosure. Privacy breaches are a regular occurrence with identity thefts, stolen credit card numbers, or exposure of financial information. Within the federal government, millions of dollars worth of equipment has been lost and the personal information of millions of veterans compromised. Melissa Hathaway, acting senior Director for Cyberspace for the National and Homeland Security Councils, in a speech last week told of an incident in which 130

automatic teller machines in 49 cities around the world were illicitly emptied over a 30 minute period.

The Wall Street Journal reported last week that the operational information for the Joint Strike Fighter – an advanced stealth-capable warplane – was breached, making it easier for our enemies to defend themselves against it. When 50 million people in eight northeast states and Canada lost power in August 2003, we got a pretty good idea of the fallout that could result from a cyber attack on the electric grid – although I hasten to add that incident was not an intentional attack but caused by broken tree limbs. Recently, we have learned of severe vulnerabilities in our electrical grid and we have read reports that foreign governments seeking to map our infrastructures have intruded into our electric systems on a grand scale.

To address these vulnerabilities, I will be introducing legislation later this week with House Homeland Security Committee Chairman Bennie Thompson.

We know our cyber infrastructure is insecure and our security capabilities are inadequate. The Government Accountability Office and

various Inspectors General have been reporting on these weaknesses for years. Last December, the Center for Strategic and International Studies issued a report, listing the vulnerability of cyber networks as one of our major national security threats.

Toward the end of the last Administration, serious thought was being given to securing government networks in a coordinated fashion. The Comprehensive National Cyber Security Initiative (CNCSI) was established last year as part of a multi-agency, multi-year plan to secure cyber networks. DHS has taken the lead on portions of the initiative through the National Cyber Security Division, which works with public, private, and international partners to secure our federal cyber assets. I am pleased that the Obama Administration's FY10 budget asks for an increase of funds to bring the National Cyber Security Division (NCSD) budget up to \$355 million. But this money must be spent wisely.

DHS also must do more to engage and include the private sector, which owns at least 80 percent of the nation's critical infrastructure, including our energy supply lines, our water systems, the nation's communications and financial networks – essentially the computerized

systems that support so much of our way of life. Given its far flung ownership and expertise, private industry must be brought to the table by DHS as we set our national cyber security priorities and improve our national cyber security defenses.

We are fortunate to have with us today some of the leading thinkers in this area who have developed excellent ideas about how to safeguard our cyber infrastructure. Stewart Baker is Former Department of Homeland Security Assistant Secretary for Policy; James Lewis is Director and Senior Fellow for the Technology and Public Policy Program at the Center for Strategic and International Studies, which issued the report I referenced earlier; Alan Paller is Director of Research at the SANS Institute; and Tom Kellermann is Vice President of Security Awareness at Core Security Technologies. Gentlemen, thank you for your attention to the subject. I look forward to our discussion.

Senator Collins.