Testimony of Senator Feinstein
Homeland Security & Governmental Affairs Committee
"Cybersecurity Act of 2012"
Thursday, February 16, 2012, 2:30 pm

Chairman Lieberman and Ranking Member Collins, thank you for holding this hearing. I want to thank both of you – as well as Chairman Rockefeller – for your leadership on this issue and your major efforts over the past two Congresses on cybersecurity.

I am pleased to join the three of you as an original co-sponsor of the "**Cybersecurity Act of 2012**," which is a comprehensive bill to improve the cybersecurity of both the private sector and the federal government.

The Growing Problem of Cyber Intrusions:

Like you, the Intelligence Committee has examined the cyber threats to our national and economic security. Just last month, at our worldwide threats hearing, the U.S. Intelligence Community's official written testimony equated cyber threats to terrorism and proliferation as the highest priority threats to our security.

FBI Director Robert Mueller testified that "***the cyber threat, which cuts across all programs, will be the number one threat to the country***."

Already, cyber attacks are doing great damage to the United States, and the trend is getting worse. Consider the following four examples, each of which is only the unclassified tip of a much larger iceberg:

- **The Pentagon's networks are being probed thousands of times daily** and its classified military computer networks suffered a "significant compromise" in 2008 according to former Deputy Defense Secretary Bill Lynn.

- In November 2009, DOJ charged 7 defendants from Estonia, Russia, and Moldova with hacking into the **Royal Bank of Scotland and stealing $9 million** from more than 2,100 ATMs in 280 cities worldwide in 12 hours.

- In 2009, Federal officials indicted 3 men for **stealing data from more than 130 million credit cards by hacking into 5 major companies' computer systems**, including 7-Eleven, Heartland Payment Systems, and the Hannaford Brothers supermarket chain.

- Finally, an unclassified report by the Intelligence Community in November 2011 said **cyber intrusions against U.S. companies cost untold billions of dollars annually and named China and Russia as aggressive and persistent cyber thieves**.

Modern warfare is already employing cyber attacks, as seen in Estonia and Georgia. And unfortunately, it may only be a matter of time before we see cyber attacks that can cause catastrophic loss of life, whether by terrorists or state adversaries.

Our enemies are constantly on the offensive and in the cyber domain, it is much harder for us to play defense than it is for them to attack. The key question is: "*What do we do about this dangerous and growing cyber threat?*"

I believe the comprehensive bill that has been introduced – the Cybersecurity Act of 2012 – is an essential part of the answer.

Improving Cyber Information Sharing (Feinstein Bill):

I'd like to speak briefly on the cybersecurity information sharing bill that I introduced on Monday, and that you have included as Title Seven in your legislation.

The goal of this bill is to improve the ability of the private sector and the government to share information on cyber threats that both sides need to improve their defenses.

However, a combination of existing law, the threat of litigation, and standard business practices has prevented or deterred private sector companies from sharing information about the cyber threats they face and the losses of information and money they suffer. We need to change that through better information sharing, in a way that companies will use, that protects privacy interests, and that takes advantage of classified information without putting that information at risk.

What Title VII: "Information Sharing" Does:

Specifically, Title VII of the Cybersecurity Act of 2012:

(1) Affirmatively provides private sector companies the authority to monitor and protect the information on their own computer networks.

(2) Encourages private companies to share information about cyber threats with each other by providing a good faith defense against lawsuits for sharing or using that information to protect themselves.

(3) Requires the Federal government to designate a single focal point for cybersecurity information sharing. We refer to this as a "Cybersecurity Exchange," to serve as a hub for appropriately *distributing* and *exchanging* cyber threat information between the private sector and the government. This is intended to reduce government bureaucracy and make the government a more effective partner of the private sector, but with protections to ensure that private information is not misused. This legislation provides no new authority for government surveillance.

(4) Establishes procedures for the government to <u>share classified cybersecurity threat information</u> with private companies that can effectively use and protect that information. This is a prudent way to take advantage of the information that the Intelligence Community acquires, without putting our sources and methods at risk, or turning private cybersecurity over to our intelligence apparatus.

<u>The Need for Data Breach Legislation:</u>

Mr. Chairman, I would like to raise one issue that is not yet included in this cyber-security package: **data breach notification.**

This is an issue I have worked on for over eight years, and it is in urgent need of attention in the Senate. My current bill – the Data Breach Notification Act – has been approved by the Judiciary Committee, and accomplishes what are, in my view, the key goals of any data breach notification legislation:

1. Notice to individuals, who will be better able to protect themselves from identity theft;
2. Notice to law enforcement, which can connect the dots between breaches and cyber-attacks; and
3. Preemption of the 47 different state and territorial standards on this issue, so companies are not subjected to often-conflicting regulation by the states.

I know that Senators Rockefeller and Pryor have a bill on this topic in the Commerce Committee, and that Senators Leahy and Blumenthal have their own bills that were reported out of the Judiciary Committee.

The differences between our approaches are not so great that we cannot work them out, and I am prepared to sit down with members of this Committee, with Senator Rockefeller, and others to find a common solution.

In sum, I look forward to the consideration of this comprehensive cyber legislation and I hope it will be taken up by the Senate soon. Thank you very much for the opportunity to testify on this important issue.