TESTIMONY OF SCOTT BORG
DIRECTOR AND CHIEF ECONOMIST, U.S. CYBER CONSEQUENCES UNIT

UNITED STATES SENATE
COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

FEBRUARY 23RD, 2010

Thank you for inviting me. My name is Scott Borg. I am the Director of the U.S. Cyber Consequences Unit. This is an independent, non-profit research institute that investigates the economic and strategic consequences of cyber attacks. We supply our results only to the U.S. government and to the public. At the US-CCU, I have had the privilege of leading an extraordinary team of cyber-security experts, economists, and other investigators, many of whom are nationally famous in their fields. This team has included Warren Axelrod, John Bumgarner, Joel Gordes, Ben Mazzotta, Michael Mylrea, Ardith Spence, Paul Thompson, Charles Wheeler, and a number of others. Since 2004, we have been visiting facilities in critical infrastructure industries and interviewing employees to determine what cyber attacks are actually possible and what their effects would be. We have been given access to the business records of large critical infrastructure corporations, so that we could analyze their dependence on their suppliers and their customers' dependence on them. We have developed powerful conceptual frameworks and analytic tools for making sense of this information.

There are three points I would like to make today:

First, cyber attacks are *already* damaging the American economy *much* more than is generally recognized.

Second, the biggest *growth opportunities* for the American economy all depend on better cyber security.

Third, in order to get the improved cyber security we urgently need, we must fix a number of broken or missing *markets*.

The greatest damage to the American economy from cyber attacks is due to massive thefts of business information. This type of loss is delayed and hard to measure, but it is much greater than the losses due to personal identity theft and the associated credit card fraud. The reason the loss from information theft is so great is that we really do operate in an information economy. The amount of value a company can create and capture is generally proportionate to the amount of information it can utilize that its global competitors can't. Education is economically important because it allows us to create and apply more information. The greater portion of the value, even in most manufactured goods, is not in the materials from which things are made, but in the information they contain. A modern automobile or airplane, from an economic standpoint, is primarily an information product.

To understand what this means, think of how a company makes money. It introduces a new product or new feature and collects a premium for it until its competitors start offering something comparable. Even after that, the company will probably still be able to make a profit on that item, because it will know how to produce it for less. When a new production facility opens, there will typically be a five to fifteen percent drop in costs each year for the first three to six years. This is because the company is learning how to do everything more efficiently. The amount by which the company's costs are lower than the costs of its competitors is normally all profit.

Now think of what happens if the company's information is stolen. The period during which it can collect a premium will be reduced to almost nothing, because the competitors will be able to offer an equivalent product right away. The profits due to lower costs will be gone, because the competitors will have all the detailed information that made the greater efficiencies possible. The competitors' costs will actually be lower than those of the victimized company, because the competitors won't have the expense of creating the information. Instead of collecting a healthy profit, the victimized company might now be struggling to survive.

Most of the other factors allowing companies to prosper can also be wiped out by information thefts. To get an idea of the effect of information thefts on the larger economy, imagine this sort of example multiplied thousands of times.

The biggest large-scale *growth* opportunities for the American economy also depend on better cyber security. This is because nearly all of the more innovative ways of creating value need information technology to be implemented efficiently.

There are eight big growth opportunities that I have been able to identify. These include things like the Flexible Re-Allocation of Capacity, which is what lies behind the smart grid and cloud computing, Mobile Information Support, which boosts efficiency with tools like electronic medical records, and Smart Products, which will allow material products, such as smart phones, to increasingly "contain services."

Examining this list reveals that each of these opportunities requires networked computers and is vulnerable to cyber attacks. An awareness of this is the main thing that has already been holding back the adoption of practices like cloud computing. More important, nearly all of these economic initiatives, including the smart grid and electronic medical records, could be brought to a screeching halt by a greater awareness of the vulnerabilities that they are introducing.

The solutions to these problems are not something that the government can directly legislate into existence. The reason is that both the information technology and the techniques employed in cyber attacks are developing so rapidly. If the government tries to mandate standards, they will be out of date—and an actual impediment to better

security—before they can be applied. This is not like fire codes in building construction, where the big changes take decades. We don't know what the minimum code for cyber security should look like four years from now.

If there is any area of the American economy that needs creative, entrepreneurial problem solving, it is therefore cyber security. Yet our markets are not currently delivering improvements in cyber security at anything like the necessary rate. In some cases, they are not delivering improvements at all.

When markets are not functioning properly, there are identifiable reasons. Sometimes companies are not being charged for all of their costs or paid for all of the benefits they produce. Other times, the individual agents are not adequately motivated to act in the long term best interests of their company. Still other times, there isn't enough information available for good market choices. There are six such reasons altogether, and each suggests possible remedies. It is these market remedies that should be at the center of our discussions on how to save our economy from the destructive effects of cyber attacks.

Thank you.