Statement of Robert L. Hutchinson
Senior Manager for Information Security Sciences
Sandia National Laboratories

United States House of Representatives Committee on Energy and Commerce
Subcommittee on Communications and Technology

March 28, 2012

Chairman Walden and Ranking Member Eshoo, and the distinguished members of the Committee; thank you for inviting me to testify before you today. I am Bob Hutchinson, Senior Manager for Information Security Sciences at Sandia National Laboratories.

Sandia is a multi-program, multi-disciplinary Department of Energy national laboratory operated by Sandia Corporation as a Federally Funded Research and Development Center. We are an independent entity sponsored by the U.S. government to provide detailed technical expertise on complex national challenges.

Sandia has over fifty years of experience protecting critical information systems against sophisticated adversaries. The Department of Energy makes its significant investment in Sandia's cyber security capabilities available to the Departments of Defense and Homeland Security, as well as other government agencies and non-federal entities. A key element of our work is to help increase the overall cyber security of public and private communications networks. Further, Sandia often functions as a hub that works at the intersection of academia, industry, and government to drive cyber innovation and advance the overall national and global cyber health.

I've been working to secure critical government computer systems—both as a researcher and as an implementer—for over 25 years, and today's testimony is based on that experience.

The most important lesson I have learned in my career is that computer systems can never be fully trusted, can never be proven free of compromise, so we must focus on finding ways to conduct business, even critical business, on machines that are presumed to be infected. We can all be victimized by countless threats in our daily lives—car accidents, diseases, theft—and yet we have found ways to manage those daily risks and move about our days. This mindset has served us well for centuries and must be applied to computer security; our focus should be on accomplishing our goals not on building and maintaining perfect computers and networks.

I would like to suggest four specific shifts in the current national approach to cyber security. Each of these suggestions implies a role for the government and a role for industry. My intention is to highlight the strengths of each of these communities and to find ways that they can reinforce each other's interests.

Number one: In recent years, the nation's cyber security approach has shifted to an almost exclusive focus on data theft. While this trend has been growing for a number of years, it understandably worsened in the aftermath of the Wikileaks intelligence theft. Our best security

analysts are being taught to focus their attention on indications that sensitive data is leaving our networks, headed into enemy hands. While data theft is a critical problem for government and for industry, I believe that our nation has diverted too many resources away from an equally, if not more, important issue: malicious data modification. As much as I worry about the theft of sensitive government data and US intellectual property, my greater fear is that an attacker will alter our data and affect our decision processes; this form of attack has not only economic consequences, but can also impact public safety and confidence. My staff and I focus much of our research on these scenarios. We must continue to worry about data theft, but not to the detriment of other cyber attack goals. The government should increase focused research and development investment on preserving data integrity.

Number two: We tend to view the stacks of mobile devices and networking components that arrive at US ports as pristine; when we discover a compromise, we strive to return devices to factory original settings. This is a fundamentally flawed security model. We don't have any idea whether our devices have been pre-compromised during design, manufacture, or distribution; we call this a supply chain attack. As an unclassified example, a few years ago, a major hard drive manufacturer was discovered to have shipped brand new hard drives with malware pre-installed. The government, in part through Sandia, has been addressing these supply chain attacks for over three decades. But commercial companies share this risk with the government. The government can help industry by informing commercial companies of our lessons learned, and helping those companies use their existing supplier relationships to begin addressing this problem where it will have the greatest impact: directly within the companies' own supply chains.

Number three: The government is taking significant steps in sharing information about cyber threats with industry; what makes this task difficult is a lack of agreement on what should be done with the shared data. We need information sharing that enables a community of stakeholders to execute a strategy. For example, can we cause an adversary to reveal his identity? Before we can achieve this goal, we need information sharing systems that respect not only data, but the strategy and rules associated with that data. A system with clear, enforced rules should enable both government and industry to benefit while allowing all stakeholders to effectively manage their own business interests and risks.

Finally, number four: The most consistent cyber security message across government and industry is that our nation has a profound shortage of qualified cyber security experts. There are many efforts to educate, train, and certify. Degrees and certifications are not enough. Cyber security is a new field of study that lacks science and engineering rigor. The best people in this field learned through practice and apprenticeship; they use judgment that is based on years of experience. The Department of Energy made this discovery over ten years ago, when they asked Sandia to build a program that’s more like a medical residency than a trade certification. Many of the people who have participated in this program have become national leaders in securing emerging technologies such as mobile device networks and cloud services. This investment has yielded greater returns than any other program that I’ve been involved in. Expanding this model so that all US cyber security professionals learn through a form of residency would result in enormous gains for national security.

Thank you for the opportunity to testify; I look forward to your questions.