OPENING STATEMENT

Ranking Member Suzanne Bonamici (D-OR)
Joint Hearing of the Subcommittees on
Energy and Research & Technology
Committee on Science, Space, and Technology

"Cybersecurity for Power Systems"
October 21, 2015

Thank you, Chairman Weber and Chairwoman Comstock, for holding this hearing, and thank you to our witnesses for participating. As many of you know, October is National Cyber Security Awareness Month, so it's a fitting time for this hearing.

We are all familiar with the increasing frequency of cyber attacks that compromise personal and business information.

At the World Economic Summit earlier this year, cyber threats made the top 10 list of most likely global risks. Lloyd's of London estimates that cyber attacks can cost businesses as much as $400 billion a year.

What we are focusing on today, however, is a different kind of cyber security. It's about securing the electric grid so a cyber attack doesn't affect grid operations, which could halt our daily lives and threaten our economic security. These attacks often gain entry through an information technology system, but, instead of taking corporate data they directly target system operations that can cause havoc and chaos.

In February of this year, an elite group of hackers broke through an electric utility's firewall and gained access to their substation controls in 22 minutes. Luckily the attack was a drill initiated at the request of the utility to test their system. But this example demonstrates what's possible.

The energy sector continues to report more cyber attacks to the Department of Homeland Security than any other critical infrastructure sector. In just one month the PJM Interconnection, which coordinates electricity transactions in 13 states and DC, experienced 4,090 documented cyber attempts to attack their system. That's more than five and a half attacks on their electrical market system per hour.

So far no publically reported cyber events have resulted in an electricity outage in the U.S. But the sophistication of attacks on industrial controls systems is increasing.

Utilities across our country are advancing energy efficiency through smart grids and programs like feed-in tariff systems. As we discuss ways to keep the grid safe, we must be mindful of doing so without inhibiting innovation.

Google, Wells Fargo, and Aetna are exploring ways to leverage employee behavior as a tool, instead of a vulnerability, to build a more secure system. From understanding how people swipe their phones, to the patterns they use when typing on a keyboard or walking, a better understanding of behavioral biometrics is opening the door to developing more cyber-secure components and processes.

The more we understand about human and social behavior, the stronger our toolbox. Rather than resting the success of our cybersecurity efforts on programs that require changes in human behavior, we might have better success if we change our technology and processes to fit the behavior of people. And the more we understand the behavior of threat actors, the better we can design protections.

So in addition to building a better technology-based firewall, we need to invest in developing a better human firewall. Our weakest link and our most resilient asset to meet the dynamic changing needs of the cyber arms race is us.

I thank each of our witnesses for being here today, and I look forward to hearing what each of you has to say.

Thank you, Mr. Chairman, and I yield back my remaining time.