Statement of the Honorable Cliff Stearns
Committee on Energy and Commerce
Chairman, Subcommittee on Oversight and Investigations
Hearing on "Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security"
February 28, 2012

(As Prepared for Delivery)

I call to order this subcommittee's second hearing on cybersecurity and critical infrastructure protection.

America's infrastructure systems have become more automated and more reliant on information systems and computer networks to operate. While our systems are more efficient, they also open the door to cyber threats and cyber-attacks. Today, the subcommittee focuses on that part of the critical infrastructure known as Smart Grid, which refers to the information technology systems increasingly incorporated into the nation's electricity networks.

Smart grid technologies are designed to lower operation costs, reduce maintenance costs, and expand the flexibility of operational control relative to the current grid system. Their operational efficiency and improved asset use is driven by advanced communication and information technologies.

I believe that we must update our electric grid with better technology integration, which is why I spearheaded the effort to secure funding for Energy Smart Florida, the largest smart grid demonstration project in the country. This initiative will invest hundreds of millions in smart grid technology and renewable energy in Florida and throughout the entire county. Energy Smart Florida will revolutionize how people use energy in their homes and enable them to make smarter choices about energy consumption and better control their carbon emissions. In addition, the widespread deployment of smart meters will provide Floridians with more reliable electrical service through an intelligent network that will be able to detect potential problems and automatically reconfigure the grid to minimize or eliminate outages.

But ask any expert in the national security field and see what keeps them up at night. They would probably tell you, as they tell me, that it is the increased possibility of a devastating cyber-attack. This threat is real and is why it is vitally important for us to do what we can to protect our critical infrastructure from these threats. We have seen in the past decade what impact both man-made and natural disasters have on our nation's utility systems. Imagine the impact of a cyber-attack to the electrical grid: How many days could hospitals operate with on-site electricity generation? How would metro rail systems operate if at all? How would we recharge our smart phones or access the internet? The goal of the Smart Grid is to improve efficiency, reliability and interoperability. An equal goal however, must be to improve upon the security controls and to minimize the impact from a man-made or natural disaster to ensure reliability and avoid such possibilities.

A recent report completed by Pike Research, estimated that utilities' initiatives to secure their infrastructure will drive increasing investments in cybersecurity systems and total roughly $14 billion from now through 2018. While DOE has emphasized investment in technologies such as smart meters, among other technologies, we want to ensure that where there is investment, there is not a cybersecurity gap. We want to emphasize that there is also investment in securing control system segments including transmission upgrades, substation automation, and distribution automation systems.

Protecting critical infrastructure is a complicated issue. We are talking about facilities and frameworks owned by private companies, and by federal, state, and local governments. They are interconnected — electricity powers water systems that cool nuclear reactors, for example. They are vulnerable to threats from a number of different sources, including nation-states, criminals, and hackers.

The issues surrounding critical infrastructure protection and security are complex. To help analyze these complexities, I am pleased to be joined by our panel of experts in their field.

Today, we will hear testimony from two witnesses at GAO: Mr. Gregory Wilshusen, Director of Information Security Issues, and Mr. David Trimble, Director of Natural Resources and the Environment. I look forward to their testimony, and getting a better understanding of their extensive work examining cybersecurity implications of the Smart Grid. I also would like to welcome Mr. Richard Campbell, of the Congressional Research Service, who has examined this very subject and we look forward to his contributions today.

As I mentioned previously, this is the Subcommittee's second hearing in this Congress on critical infrastructure protection and cybersecurity. The purpose of this hearing, in particular, is to get an overview of Smart Grid cybersecurity, and how it is working and what can be done better. It is my intention to call DOE and possibly other stakeholders to a future hearing for further consideration of Smart Grid security.

I have enjoyed working with Ranking Member DeGette and the Minority in these matters and look forward to working with her on overseeing cybersecurity issues.

I look forward to hearing the perspectives of our expert witnesses about the safety of this vital part of critical infrastructure, and whether we are taking the right steps to protect them from cyber risks and threats.